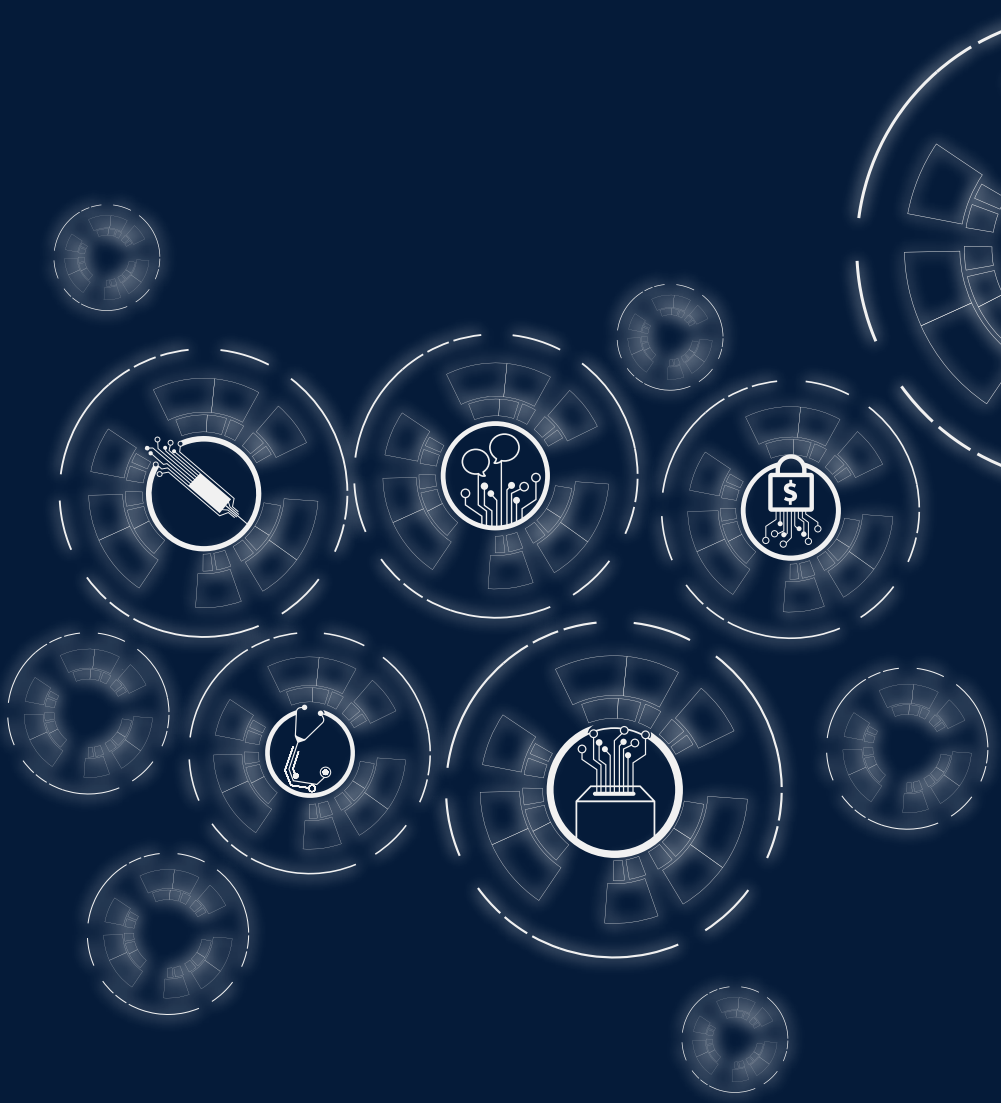


The Oxford Process on International Law Protections in Cyberspace:

A Compendium

OXFORD INSTITUTE FOR
ETHICS, LAW AND
ARMED CONFLICT

The Oxford Process on International Law Protections in Cyberspace:

A Compendium

The Oxford Process is based at the Oxford Institute for Ethics, Law and Armed Conflict (ELAC) whose work on international law and cyber operations is supported financially by Microsoft Corporation and the Government of Japan. The views expressed in the papers contained in this publication do not necessarily reflect those of the sponsors of the Oxford Process.

Microsoft

JAPANGOV
THE GOVERNMENT OF JAPAN

Table of Contents

Introduction

The Oxford Process on International Law Protections in Cyberspace, convened by Professors Dapo Akande and Duncan B. Hollis, is an initiative of the Oxford Institute for Ethics, Law and Armed Conflict (ELAC) at the Blavatnik School of Government, University of Oxford. It was set in motion in May 2020 in partnership with Microsoft and the Government of Japan.

The Oxford Process is a collaborative effort of leading international legal experts from across the globe to build consensus around international law protections in cyberspace. It is aimed at identifying and clarifying the rules of international law applicable to cyber operations targeting particular objects of protection or using particular methods. In doing so, it seeks to move beyond the general assertion that international law applies in cyberspace to understand how it does so in real-world situations. The Process responds to the most urgent problems facing the international community with respect to information and communications technologies and their cyber environment.

The present Compendium includes the five Oxford Statements on International Law Protections in Cyberspace – the Oxford Statement on the International Law Protections against Cyber Operations Targeting the Healthcare Sector, the Oxford Statement on Safeguarding Vaccine Research, the Oxford Statement on Foreign Electoral Interference through Digital Means, the Oxford Statement on the Regulation of Information Operations and Activities and the Oxford Statement on the Regulation of Ransomware Operations, as well as the posts accompanying the Statements, reports from every workshop convened under the auspices of the Process, and related statements and publications by members of the Oxford Process team and workshop participants.

Background

Despite the promises of geopolitical conciliation and the eradication of both poverty and violence that defined the end of the 20th century, the world entered the second decade of the 21st century on the verge of a global pandemic and a war of aggression in Europe. The last few years have also witnessed multiple armed conflicts lingering across continents, large-scale human rights violations and an overall erosion of trust in domestic and international institutions. And even as the old threats to international peace and security remain, new ones have emerged. Cyber threats are on the rise, as we witness the normalisation of cyber insecurity. Since the start of 2020, operations conducted via information and communications technologies (ICTs) have targeted, among many others, electric power utility companies and telecommunication services in Latin America, hospitals and vaccine research facilities across Europe and Asia, governmental structures and the financial sector in many African countries, essential services, such as water and energy supply, in North America and the Asia-Pacific region, as well as ICT companies mostly based in the United States. These cyber threats know no frontiers, and they imperil the security of States, private entities, and individuals worldwide.

Our increasing dependence on the Internet and other digital technologies means that hardly any sphere of life has remained untouched by this constant stream of nefarious cyber activity. Attacks crippling the functioning of hospitals, research institutes and water filtration plants endanger lives and livelihoods. Privacy is becoming more of an aspiration than a reality, with personal data compromised following IT supply chain attacks, or exposed through hacks on social media platforms or dating apps later shared on the Darknet. Information campaigns tamper with electoral processes, manipulating and intimidating voters while a raging infodemic has accompanied the COVID-19 pandemic. Amplified by inter-connectivity and digital tools, manipulated information travels fast and reaches far. Ransomware, insidious and inherently coercive, drains and disrupts businesses and public institutions. Looking at the operations from the past two years, little, if anything, seems to be off limits.

What consequences flow from this rise and proliferation of harmful cyber operations?

First, trust, a key component of any functioning society, including the international one, is now under attack. Cyber activities undermine trust in

institutions, such as humanitarian organisations, essential cybersecurity protocols, like software update mechanisms, electoral processes, and even science itself.

Second, although a matter of mere speculation in the past, direct harmful effects, such as injury, damage, disruption, psychological distress are now becoming clearly observable in the aftermath of cyber operations.

Third, the rise and proliferation of harmful cyber operations have also led to their increased sophistication. Packaged malware is becoming harder to detect on targeted systems, while malicious exploits evade cyber defences in novel ways.

Fourth, to counter these trends, more public and private resources have necessarily been directed towards the patching of vulnerabilities, building robust cybersecurity, and awareness campaigns on cyber hygiene. Ensuring a secure cyberspace comes at a high financial cost and may require further diversions of funds from other areas that are important to public life. Such trade-offs notwithstanding, there is a growing awareness and acceptance that cyber security is a precondition for the normal functioning of societies.

A fifth and final consequence is that, in a space that is becoming increasingly uncertain due to evolving risks of harm, the need for *legal certainty* is pressing and acute.

As the March 2021 Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the context of International Security (OEWG) concluded, 'additional neutral and objective efforts to build capacity in the area of international law' are needed to deepen understanding of how international law applies to the use of ICTs information and communication technologies. Similarly, in its July 2022 report, the OEWG recognised that '[c]apacity-building efforts on international law could be strengthened and could include workshops and training courses.' Simply put, the dramatic rise of cyberthreats has increased the demand for clearly stated rules of international law.

In a time of distress and insecurity, when State actors flagrantly breach fundamental rules of the international order and non-State actors capitalise on societal vulnerabilities, the Oxford Process on International Law Protections in Cyberspace clearly responds to the UN call and reaffirms our faith in and commitment to international law and the international system.

Both states and other stakeholders have coalesced around the view that international law – a growing regulatory framework governing international and domestic affairs – has a crucial role to play in ensuring legal certainty, as well as preventing and redressing harmful cyber behaviour. Greater clarity on the protective reach of international law, via its prohibitions, permissions, and requirements, can exercise a pull towards compliance by all actors within this system. That compliance can, in turn, facilitate reduction in harmful cyber activities, as well as prevention, mitigation and redress for harms caused.

In a time of distress and insecurity, when State actors flagrantly breach fundamental rules of the international order and non-State actors capitalise on societal vulnerabilities, the Oxford Process on International Law Protections in Cyberspace clearly responds to the UN call and reaffirms our faith in and commitment to international law and the international system.

Over the past two years, the Oxford Process on International Law Protections in Cyberspace has sought to respond to this growing need, establishing itself as one of the key neutral capacity-building initiatives aimed at the clarification of international law. It represents an effort to deepen understanding on the application of international law and to provide clarity on how this body of law governs and prohibits a range of cyber threats. Unlike other legal capacity-building initiatives, the Oxford Process focuses on concrete instances of harmful cyber operations as a way to reach agreement on their international regulation. After all, in every challenge lies an opportunity. The importance of this approach was recognised in the July 2022 OEWG Report, which noted that the Group 'could convene discussions on specific topics related to international law', and that '[s]uch discussions should focus on identifying areas of convergence and consensus.'

As an academic effort with government and industry support, the Oxford Process also reflects the importance of State engagement with multiple stakeholders, emphasised in the May 2021 consensus report of the Group of Governmental Experts on Advancing Responsible State behaviour in cyberspace in the context of international security (GGE). Such multi-stakeholder efforts at defining norms of international law in this area, the GGE highlighted, are 'critical to bridging existing divides within and between States on policy, legal and technical issues relevant to ICT security.'

The Oxford Process at a glance

The Oxford Process on International Law Protections in Cyberspace is an initiative of the Oxford Institute for Ethics, Law and Armed Conflict (ELAC) at the Blavatnik School of Government that was set in motion in May 2020 in partnership with Microsoft and the Government of Japan. In the ensuing months, the Process has emerged as a collaborative effort among dozens of international legal experts from across the globe, aimed at identifying and clarifying the rules of international law applicable to cyber operations targeting particular **objects of protection** or using particular **methods**.

The goal of the Oxford Process is to move beyond the simple assertion that international law applies in cyberspace to clarify exactly how it does so. The Oxford Process provides a **platform for multi-stakeholder discussions and articulation of points of broad consensus on international legal rules.** Over the course of 2020, 2021 and 2022, the Process has produced a number of major outputs, including five **Oxford Statements on International Law Protections in Cyberspace,** each of which articulates short lists of consensus protections understood to apply under existing international law. More than a hundred international lawyers from all continents have endorsed each of these Statements. The Statements have subsequently earned recognition by both public and private fora grappling with related problems. **Today, hardly any inter-governmental meeting, private sector conference or academic workshop dealing with the regulation of cyberspace goes by without a discussion of the work done within the auspices of the Oxford Process. This is because the Process fills an acute need for clear and strong messaging on the application of international law to cyberspace.**

The Oxford Process provides a platform for multi-stakeholder discussions and articulation of points of broad consensus on international legal rules.

History

In May of 2020, ELAC hosted a two-day virtual workshop, co-sponsored by Microsoft and the Government of Japan, entitled 'Applying International Law in Cyberspace: Protections and Prevention'. This workshop occurred at a time when **cyber operations against the healthcare sector were intensifying,** during a particularly worrisome and pernicious global pandemic. During the very rich workshop discussions, the participants examined a wide range of relevant international legal rules, both negative (that is, obligations to refrain from doing something) and positive (that is, obligations to do something or take certain steps to achieve certain results). Even in a virtual room filled with international lawyers – each with their own take on the existence and content of particular rules – agreement emerged in substance: international law prohibits cyber operations by States that have serious adverse consequences for essential medical services in other states. Divergences arose regarding how the participants reached this conclusion, with different experts placing reliance on a range of principles and rules, such as non-intervention, sovereignty, international humanitarian law, and human rights. But despite differences on the precise legal route taken, there was widespread agreement on the nature of the prohibited acts and the coverage of international legal protection, *i.e.* the substance of prohibited or required State behaviour.

It was this realisation – of agreement on protective coverage – that led to the first Oxford Statement elaborating points of consensus on the protection of the healthcare sector. The ensuing four statements — the Oxford Statement on **Safeguarding Vaccine Research**, the Oxford Statement on **Foreign Electoral Interference through Digital Means**, the Oxford Statement on the **Regulation of Information Operations** and Activities and the Oxford Statement on the **Regulation of Ransomware Operations** – followed the same approach of identifying substantive commonalities.

These Statements reflect the uniqueness of the Oxford Process with its singular focus on clarifying the rules of international law applicable to cyber operations targeting particular **objects of protection** or using **particular methods**. Beyond the five workshops that led to Statements, the Process also convened additional events to delve deeper into

particular legal issues permeating the Statements: 1) a workshop on 'Cyber Due Diligence Obligations in International Law: Theory and Practice', which unpacked the due diligence provisions incorporated in each of the Five Statements); 2) a workshop focused on the protection of IT Supply Chains; and 3) a workshop on responses to unlawful cyber operations, with a particular emphasis on countermeasures. Each of these events generated an Oxford Process Report, detailing the workshop presentations, discussions, and, most importantly, areas of agreement and disagreement.

Methodology

The methodological approach of the Oxford Process is its distinctive feature, and one which clearly distinguishes it from other academic initiatives looking at the international legal regulation of cyber operations. This approach has four main characteristics: it 1) is based on consensus between participants; 2) inquires into the application of international law to specific objects and methods; 3) responds to urgent problems facing the international community; and 4) elevates the role of positive obligations.

1) Articulating points of consensus

The Oxford Process articulates points of consensus (the 'low-hanging fruit', or the common denominator of positions) without necessarily being prescriptive about the particular principles or rules of international law that underlie conclusions on the scope of legal protection. **In this way, the emphasis is on unity, not on differences.**

2) International law applied to specific objects and methods

Rules of international law are not discussed in the abstract. The Oxford Process looks at specific objects and areas of protection, as well as particular methods of conducting cyber operations. This is important, as the means and ends of cyber operations inform and concretise the ways in which international law regulates particular conducts. For this reason, the first Oxford Statement focused on healthcare, the second

on vaccine research, the third on electoral processes, the fourth on information operations and activities, and the fifth on ransomware. The first three Statements centred around specific objects or areas of protection, while the last two transitioned to identifying particular limitations on methods of cyber operations.

3) Responding to urgent global problems

Guided by discrete needs triggered by specific events, the Oxford Process is grounded in the current reality of cyber operations and cyber-related harms. Hence, technical and policy experts are often invited to present at the workshops and encouraged to actively participate in the discussions. This wealth and diversity of real-life and real-time expertise facilitates the connection between international legal rules and the reality of cyber operations, thus allowing a deeper understanding of the harm that such operations can cause and the measures that can and are being taken to prevent, mitigate and redress such harm.

For example, at the very start of the July 2020 workshop aimed at clarifying the protection of vaccine research, a cybersecurity expert introduced the participants to the types of harm that accompany even the mere entry into networks that contain trial data on vaccines (including the possibility of needing to fail that trial), challenging international lawyers' conventional wisdom that losses of confidentiality alone can never cause a loss of integrity in the targeted system. This led to a Statement that identified the act of penetration into vaccine research systems or databases as harmful in itself and, thus, entailing particular legal consequences. Similarly, during the IT Supply Chains workshop, the group, guided by an expert from the private sector, dived into the mechanics of the SolarWinds hack, including the way in which the malware became part of the update build and received the provider's digital certificate. All of these details shaped the discussions, as they clarified the precise form that harmful cyber operations now take and the precise types of harm to which they can give rise.

4) Elevating the role of positive obligations

The majority of earlier efforts to understand and assess the application of international law to cyberspace emphasized international law's restrictive character (i.e., the prohibition on the use of force, the duty of non-intervention). Without undermining the importance of these prohibitions, the Oxford Process has brought equal attention to the requirements international law may impose on States, whether as targets of nefarious cyber activity, or as part of the international community as a whole. This has included a particular emphasis on the role international human rights law may play in providing protections online.

From a procedural standpoint, each Oxford Statement is drafted and revised following careful research, often reflected in background papers, rich and rigorous workshop discussions, as well as subsequent, additional feedback received from workshop participants. Once a Statement is finalised, it is opened for signature, first by the workshop participants and previous Signatories. Then, the Statement is publicised through various academic and media channels, including on the blog of the *European Journal of International Law (EJIL:Talk!)* and on the blogs *Opinio Juris* and *Just Security*. These publications not only disseminate the content of each Statement but also invite other international lawyers to sign them. In short, all Statements followed the same five-stage process: convening of workshop → discussions → emerging consensus → consensus embodied in a brief Statement → publication.

Substantive features of the Process

A strong substantive focus underlies and defines the Oxford Process. Beyond articulating applicable areas of international law and specific rules, it seeks to provide States and other stakeholders with concrete guidance on what behaviour is expected from them. Three substantive features flow from this goal. First, the Process clarifies not only negative, but also positive obligations under international law, placing

the latter front and centre in ensuring the protection of essential objects, services and processes. Second, it seeks to identify the rules applicable not only to states, but also to other actors bound directly by international law. Third and finally, it is comprehensive in that it examines both general and specific international obligations, including rules and principles applicable in both peacetime and times of armed conflict.

Clarifying positive obligations

The Oxford Process focuses not only on prohibitive rules of international law, but also on rules that require states to take particular positive steps to prevent, mitigate and redress a range of cyber harms. Both types of rules receive equal attention and are given equal importance. All five Oxford Statements shed light on the general scope of positive obligations under international law, while at the same time detailing concrete measures that states could adopt to fulfil these obligations. For instance, the Oxford Statement on the Regulation of Ransomware Operations concluded that

> *'States must take measures to protect the human rights of individuals within their jurisdiction from harmful ransomware operations, including when such operations are carried out by other states and non-state actors. To discharge this obligation, states may, among other measures, prohibit ransomware by law, take feasible steps to stop ransomware operations, mitigate their effects, investigate and punish those responsible, as well as prevent and suppress ransom payments to the extent possible. Where such protective measures interfere with other human rights, they must conform with applicable legal requirements, such as legitimate purpose, legality, necessity, proportionality and non-discrimination.'*

The Process takes a practical approach to the application of positive obligations, whilst highlighting that positive measures must not themselves be used as a justification for breaches of international

law. Thorough and rigorous research on obligations containing a due diligence standard has accompanied the Oxford Process from its inception, with insights finding their way both into the Oxford Statements and separate workshops and publications.

Looking beyond States

States are not the only actors bound directly under international law. Mindful of this, and of the importance of clarifying the obligations of all relevant actors, the Oxford Statements have consistently outlined obligations that bind individuals and parties to an armed conflict (not only States parties but also non-State actors). For instance, the Oxford Statement on International Law Protections Against Cyber Operations Targeting the Health Care Sector concluded that

> *'5. During armed conflict, international humanitarian law requires that medical units, transport and personnel must be respected and protected at all times. Accordingly, parties to armed conflicts: must not disrupt the functioning of health-care facilities through cyber operations; must take all feasible precautions to avoid incidental harm caused by cyber operations, and; must take all feasible measures to facilitate the functioning of health-care facilities and to prevent their being harmed, including by cyber operations.*
> *6. Cyber operations against medical facilities will amount to international crimes, if they fulfil the specific elements of these crimes, including war crimes and crimes against humanity.'*

General and specific protections in times of peace and armed conflict

The Oxford Process seeks to provide a comprehensive picture of protections under international law. This means that the legal inquiries into the ways in which international law applies to particular objects and methods extend across general and specific rules applicable in peacetime and armed conflict. The starting point is that existing international law as a whole and by default applies to ICTs, without the need to craft new treaty rules or identify cyber-specific State practice and *opinio juris*. Each of

those legal inquiries is then tailored to the specific context of application. For example, in the Oxford Statement on the Regulation of Information Operations and Activities, it was concluded that

> *'The conduct of information operations or activities in armed conflict is subject to the applicable rules of international humanitarian law (IHL). These rules include, but are not limited to, the duty to respect and ensure respect for international humanitarian law, which entails a prohibition against encouraging violations of IHL; the duties to respect and to protect specific actors or objects, including medical personnel and facilities and humanitarian personnel and consignments; and other rules on the protection of persons who do not or no longer participate in hostilities, such as civilians and prisoners of war.'*

Outputs

The outputs of the Oxford Process now take a variety of forms. The five Oxford Statements referenced in the previous sections spell out, in a clear and concise way, consensus protections under existing international law. In addition to the Statements, the Oxford Process produces Reports outlining the discussions that have taken place during the various workshops. Moreover, a wide array of background papers and blog posts have been created for, or inspired by, the themes and conversations in the various Oxford Process workshops.

Though not written outputs per se, the workshops convened by the Oxford Process are a 'product' in and of themselves, as they provide a platform for dialogue across multi-stakeholder groups. Through these workshops, the Oxford Process has created its own ever-expanding community of experts. Furthermore, the workshops have served as a catalyst for further conversations on international legal protections, including areas in which differences of opinion persist as well as areas that might benefit from further elaboration or more effective regulation.

Each workshop has also spurred a search for the next topic for which the governing norms should be identified. For instance, the first workshop on the protection of the healthcare sector against malicious cyber operations prompted a more specific workshop on vaccine research and development that was convened two months after the first. Similarly, the workshop on foreign electoral interference through digital means created momentum for a subsequent workshop on the broader issue of information operations and activities.

The Oxford Process reflected in external events, processes and initiatives

Although the Oxford Process was initiated less than two years ago, it has already carved out a unique space for itself, becoming one of the most prominent and referred to initiatives when it comes to the international legal regulation of cyberspace. Support for the Oxford Process has come from legal experts around the world, including former judges of the International Court of Justice, United Nations (UN) Special Rapporteurs, and States' representatives. Each Oxford Statement has been signed by more than a hundred international lawyers – a significant feat in an area where international legal regulation is so heavily contested.

Many UN events and processes over this past year and a half have featured discussions of the Oxford Process as an important and meaningful initiative in the area of cyber regulation. The first two Oxford Statements on the healthcare sector were cited during two Arria Formula Meetings on cybersecurity at the UN Security Council, with the Acting Assistant Secretary-General for the UN Office for the Coordination of Humanitarian Affairs referring to these Statements in the context of important initiatives aimed at addressing how international law applies to cyber operations. **The Process is mentioned in key UN documents, such as the 2021 report of the UN Office on**

the Coordination of Humanitarian Affairs, 'From Digital Promise to Frontline Practice: New and Emerging Technologies in Humanitarian Action'. The Oxford Process also features prominently at the State level, with discussions on the Oxford Statements accompanying the release of national positions on the application of international law to cyberspace.

Beyond these important acknowledgments, members of the Oxford Process team are now regularly invited to present at various events in the sphere of cyber regulation including those associated with the Paris Call for Trust and Security in Cyberspace and the Internet Governance Forum, as well as sessions with representatives of the Organization of American States, the African Union, and the European Union, alongside State-organised workshops on particular areas of protection, such as Slovenia's sponsorship of discussions on protecting water, energy, healthcare and financial services, and Mexico's Regional Consultation of Latin American States on International Humanitarian Law and Cyber Operations during Armed Conflicts, co-hosted with the International Committee of the Red Cross. The Oxford Process was also the subject of a dedicated side event during the December 2021 meetings of the OEWG, with two UN Under-Secretary Generals welcoming the Process, its place and impact on State positions and the work of inter-governmental groups.

The Oxford Process is now firmly established in the international legal scene. As a norm-identification and interpretation process in a critical and fast-moving area, it complements other important initiatives, such as the UN GGE, OEWG, and the Tallinn Manuals, by adding its own unique approach to clarifying and spelling out existing protections.

Simply put, the Oxford Process is now firmly established in the international legal scene. As a norm-identification and interpretation process in a critical and fast-moving area, it complements other important initiatives, such as the UN GGE, OEWG, and the Tallinn Manuals, by adding its own unique approach to clarifying and spelling

out existing protections.

Who is behind the Oxford Process?

The Oxford Process is convened by Professor Dapo Akande (University of Oxford) and Professor Duncan B. Hollis (Temple University). Since 2020, a small core team has been working on both substantive issues and the planning and organisation of events. The team comprises Professor Harold Hongju Koh (Yale Law School), Dr Antonio Coco (Essex), Dr Talita Dias (Oxford), Mr James O'Brien and Mr Nikhil Sud (Albright Stonebridge Group),[1] Dr Priya Urs and Ms Tsvetelina van Benthem (Oxford).

Beyond this core team, however, it is the thoughts, ideas, effort and time of hundreds of people that have made the Oxford Process what it is today. All Oxford Process workshops bring together a wealth of expertise from different sectors and disciplines. Initially, the workshops attracted primarily academics but, gradually, the composition of the events changed, with the latest ones being increasingly attended by representatives of States, international and non-governmental organisations. The participating international legal experts hail from the widest range of geographic regions and legal systems: experts come from all six inhabited continents – a testament to the importance of the topics reviewed, the global demand for this kind of norm-identification initiative, and a basis for the diverse and representative discussions and outputs produced by the Process. Additionally, the Oxford Process' core team, its workshop participants and Statement signatories boast a significant presence of female experts – an important feat given the' under-representation of women in the area of technology.
The Process also bridges other gaps by bringing together different generations of scholars and practitioners, and giving a prominent role to early-career researchers.

1 Mr James O'Brien and Mr Nikhil Sud were part of the core team in 2020 - 2021.

Looking ahead

The Oxford Process is a process in more ways than one. First and foremost, it is a process of clarifying how international law applies to specific objects and methods of cyber operations. Second, it is also a process of garnering consensus by its own distinctive methodology, through which an epistemic community is established and continuously expanded through repeated dialogue. Third, it is a process of combining expertise from different legal areas, while maintaining the rigorous disciplinary methodology for identifying, interpreting and applying international law. Fourth, it is a process committed to international law as a protector of objects, services and processes that are essential for the life, livelihood and dignity of individuals. With each workshop and Statement, the Process affirms that international law is not just an apology for power. Rather, it expressly protects from harmful cyber operations the objects and sectors needed for the preservation and development of human life, health, privacy, expression, including the effective functioning of domestic institutions and essential services. Fifth and finally, it is a process of highlighting the benefits of collaboration, of debating, of navigating disagreements to discern points of consensus, of having all relevant stakeholders actively engaged and committed to a robust system of international legal protections.

Describing the fast-moving landscape of international legal rules in cyberspace is like describing what one sees from a moving train: the landscape changes as quickly, if not more quickly, than one can describe it. Such dynamic changes make the identification and application of international law challenging, but all the more necessary. In the future, the Oxford Process will continue to advance its mission of clarifying international legal rules in their application to the cyber context and responding to the most pressing problems of the day. One way of advancing this mission is to share, in an accessible way, all that has already been achieved through the Process in its first two years. This is the aim of the present Compendium. It contains all the Oxford

Statements and their Signatories, the posts accompanying their publication, the reports of all workshops, and the related publications.

Committed to ongoing dialogues with States and other stakeholders, the Oxford Process team will continue to engage with and support international processes, build capacity, expand its community of experts, seek consensus among diverging views, and respond to the evolving cyber landscape.

'The Secretary-General, in his report on "Our Common Agenda", described the internet as a "global public good that should benefit everyone, everywhere", but warned that the "potential harms of the digital domain risk overshadowing its benefits". The Secretary-General pointed to "serious and urgent ethical, social and regulatory questions" which confront us, "including with respect to the lack of accountability in cyberspace", and that "it is time to protect the online space and strengthen its governance". Increased reliance on information and communications technologies has exacerbated vulnerabilities, creating opportunities for malicious exploitation. Cyber security incidents, including some of serious concern, continue to be reported. Therefore, it is of vital importance that there are venues to discuss the application of international law in cyberspace, such as the Oxford Process, which gathers international law experts with the aim of identifying and clarifying the rules of international law applicable to cyber operations.'

Miguel de Serpa Soares
Under-Secretary-General for Legal Affairs and United Nations Legal Counsel

Image credit: Freepik.com

Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond

Written by Dapo Akande, Antonio Coco and Talita de Souza Dias

Published on EJIL:Talk!, 5 January 2021

In the past few years, a growing number of states have expressed their official positions on the applicability of international law in cyberspace. Most recently, New Zealand and Israel shared their own views on the topic to beef up the crowd. Initiatives of this kind are welcome and contribute to the gradual clarification of the extent to which international legal rules govern activities in the ever-evolving and still mysterious 'cyber domain' or 'sphere'.

As things stand, there is widespread agreement that international law applies in cyberspace. This view can be confirmed not only on the basis of numerous position papers by individual states, but also by looking at the outputs of multi-lateral fora, such as the UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (GGE) and the UN Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG, see Revised Pre-Draft Report, § 7). Thus, it appears that the main focus of ongoing debates has now moved to understanding how existing international law applies in cyberspace — an effort which has been spearheaded by numerous civil society and academia-led initiatives like the Tallinn Manual 2.0 and the Oxford Process.

However, despite the general acknowledgment that international law applies to cyberspace, doubts have been raised about the extent to

which existing international rules or principles apply to this new area of state activity. In a non-negligible number of occasions, some governments and scholars have suggested that particular international legal obligations do not apply in cyberspace. This idea seems to be premised on two mutually reinforcing assumptions. First, that existing international law can only apply in cyberspace if substantiated by sufficient evidence of domain-specific state practice and opinio juris. This search for cyber-specific practice and opinio juris is then backed with calls for more national statements on how international law applies to cyber operations. Second, in some cases, standards of conduct which actually reflect existing international obligations under general international have been framed, in the context of cyberspace, as 'voluntary, non-binding, norms of responsible state behaviour'. For example, the 2015 UN GGE Report (para. 13(c)) affirms that 'States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs'. This so-called 'voluntary' or 'non-binding' norm, in fact, refers to what the International Court of Justice referred to in the Corfu Channel case (UK v Albania, p .22) as 'every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States.' This obligation is one to act with due diligence and has come to be described as such. However, for some, the implication of putting a norm into the basket labelled 'voluntary, non-binding' is that the corresponding rules or principles have not yet developed or crystallised for cyberspace, or that this 'domain' has been carved out from the scope of said obligations. This blog post seeks to challenge these two assumptions.

Is it necessary to prove 'new' or specific state practice and opinio juris for existing international law to apply in cyberspace?

The first premise is commonly grounded in the idea that cyberspace is a 'new (virtual) domain' or field of activity and, as such, like the physical domains of air, land, sea and outer space, requires specifically-tailored rules. Israel's Deputy Attorney General put the argument more subtly and more persuasively, when he stated that:

> *"It cannot be automatically presumed that a customary rule applicable in any of the physical domains is also applicable to the cyber domain. The key question in identifying State practice is whether the practice which arose in other domains is closely related to the activity envisaged in the cyber domain. Additionally, it must be ascertained that the opinio juris which gave rise to the customary rules applicable in other domains was not domain-specific. Given the unique characteristics of the cyber domain, such an analysis is to be made with particular prudence, as it is very often the case that relevant differences exist."*

It is correct that there are cases where practice or opinio juris indicates that the application of a rule is limited to a particular context or to a specific type of activity. For example, the practice or opinio juris relating to obligation of states to respect freedom of navigation in the high seas is restricted to the high seas. It does not guarantee freedom of navigation throughout the seas, nor does it oblige states to guarantee freedom of movement elsewhere.

However, in the absence of a limitation to a particular context or type of activity, or where the previous expression of a rule (including the opinio juris and the practice) is general, there is nothing in international law that suggests that one must seek to ascertain whether a rule applies across 'domains'. For example, it is prohibited for states to arrest the serving head of another state. It matters not where the arrest takes place. To take another example, in the course of an armed conflict, it is prohibited for states to direct attacks against civilians. Again, it matters not where the civilians (or the attackers) are or what weapons are used.

The idea that international law applies to 'domains' seems to be derived from the context of armed conflict where the concept 'serves as a fundamental organizing idea, reflecting the way we conceptualize the battlefield and categorize actions taking place during armed conflict.' (McCosker, 'Domains of Warfare, in Saul & Akande (eds.) Oxford Guide to International Humanitarian Law, 2020, p. 97). However, even in that

context, it is important to recall that 'much of IHL is not domain-specific and applies generally' (McCosker, p. 78). The same is true of the law relating to the use of force. It is prohibited to use force against other states and no inquiry needs be made about the 'domain' in which a state using force is acting. In sum, we should be sceptical about a supposition that the application of international law rules is 'domain' specific.

In any event, there are good reasons to question that cyberspace is a new 'domain' requiring domain-specific state practice and opinio juris. The term 'cyberspace' is misleading in that cyber activities, whether carried out by states or non-state entities, do not occur in a new, virtual space. Rather, what we often call 'cyberspace' is nothing more than a set of information and communications technologies that enable individuals to exchange and process information more efficiently, such as the Internet and other networks. As much as software, code and data play a significant role in how these technologies operate, they are necessarily made up of physical components or hardware, such as cables, satellites, radio waves, computers and their millions of silicon circuits, as well as the individuals who build, control and use software, hardware and data. Likewise, even if these multifaceted physical components cross national borders to create an imaginary 'global information space', as encapsulated in terms such as 'The Cloud', 'World Wide Web', or 'Virtual Reality', these remain very much grounded in tangible physical infrastructure as well as human beings of flesh and bone that are located somewhere in the world.

That cyberspace is nothing more than a set of technologies was already reflected in the language used in the various GGE reports as well as the OEWG's mandate and documents, which refer precisely to 'information and communication technologies (ICTs)'. Thus, when it comes to 'cyberspace' or 'cyber operations', it is more accurate and appropriate to frame questions of applicability of international law to new technological developments. After all, online resources and activities are not an end

in themselves, but a means to achieve different aims or effects that will usually manifest themselves, in different ways, in one or more of the traditional physical domains.

In international as in domestic law, the fact that human beings have developed new technologies over time, such as trains, cars, telephones, televisions, and mobile phones, does not mean that these create new 'domains' or 'spaces' which cannot be subject to existing legal rules or principles, such as tort or criminal law. The International Court of Justice recognised as much in its Nuclear Weapons Advisory Opinion (§§ 39 and 86). Similarly, in its Draft articles on Prevention of Transboundary Harm from Hazardous Activities (154, Commentary to Draft Article 3, para 11), the International Law Commission noted that new technologies are also subject to positive duties to prevent transboundary harm. In 2020, UN member states involved in the OEWG explicitly 'confirmed that measures to promote responsible State behaviour should remain technology-neutral, underscoring that it is the misuse of such technologies, not the technologies themselves, that is of concern' (§ 21).

This 'tech-neutrality', in turn, means that existing international law writ large regulates state conduct carried out through ICTs, at least by default and to the extent relevant. International legal rules or principles of general applicability, i.e., applicable under general international law to all types of state activity in the relevant circumstances, such as the prohibition on the use of force, non-intervention, the Corfu Channel rule of 'due diligence', international human rights law and international humanitarian law, thus, do not need further proof of applicability to ICTs or other new technologies via specific state practice and opinio juris 'in cyberspace'. Their scope is sufficiently broad to be interpreted and applied to ICTs. It is the burden of those advocating for ICTs' exclusion from their scope to present evidence that states, in their general practice accepted as law, have actively carved out ICTs.

This conclusion does not deny that, when applying general rules of existing international law to new technologies, some loose ends may need to be tied and adjusted with best implementation practices to account for certain specific features, such as the unprecedented speed, reach and transboundary nature of ICTs. That notwithstanding — and in line with the views expressed on the issue by an overwhelming majority of States — the starting point is the applicability of existing international law, rather than a legal vacuum. As the Czech Republic has recently pointed out, general international law's full applicability and flexibility are particularly important vis-à-vis ICTs, given their rapid development and the difficulty for new and detailed treaty instruments to keep up to such speed (at page 2).

Do 'voluntary non-binding norms' replace established international rules?

This leads us to the second question outlined above: the relationship between the so-called 'voluntary, non-binding norms' of responsible state behaviour, especially those articulated in the 2015 GGE Report, and existing international law, subsequently endorsed by the UN General Assembly by consensus (§ 1-2(a)). The fact that the report distinguishes between the application of international law to ICTs and 'voluntary, non-binding norms' might at first glance be taken as an argument that none of the latter 'norms' are to be complied with as a matter of legal obligation. Indeed, some of those norms do not reflect binding international law obligations. However, some of them do use, explicitly or implicitly, the language of law. Reference has already been made to the norm that states 'should not knowingly allow their territory to be used for internationally wrongful acts using ICTs' — the due diligence obligation which derives from the rule of law set out by the ICJ in the Corfu Channel case. Even more explicit is the norm in para 13(f) of the 2015 GGE Report, affirming that 'a State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure …' This is a norm maintaining that states should not act contrary to their international obligations.

Could it be that certain well-established rules of international law have been demoted to non-binding recommendations by effect of the GGE work? Is it possible that though these rules are generally applicable, they do not survive as legal obligations in the cyber context because states have chosen to regard them, in that context, as only voluntary and non-binding? This may be the assumption that undergirds the recent statements mentioned at the beginning of this post, for instance as they relate to the concept of due diligence (see New Zealand, §§ 16-17; and the speech by Israel's Deputy Attorney General Schondorf). However, this argument fails to observe that the articulation of these norms is without prejudice to states' rights and obligations under international law (see Finland's February 2020 OEWG Statement). Indeed, §10 of the 2015 GGE Report make is clear that these 'norms do not seek to limit or prohibit action that is otherwise consistent with international law.' As eloquently put in the latest OEWG Revised Pre-Draft Report:

> *'Voluntary, non-binding norms reflect the expectations of the international community and set standards regarding the acceptable and unacceptable behaviour of States in their use of ICTs. They play an important role in increasing predictability and reducing risks of misperceptions, thus contributing to the prevention of conflict. Norms do not replace or alter States' obligations under international law, which are binding, but rather provide additional specific guidance on what constitutes responsible State behaviour in the use of ICTs. […] Alongside international law, voluntary non-binding norms complement confidence-building and capacity-building measures and related efforts to promote an open, secure, stable, accessible and peaceful ICT environment.' (at page 7, Introduction to Section D)*

and

> *'In their discussions at the OEWG, States reiterated that voluntary, non-binding norms of responsible State behaviour are consistent with international law and with the purposes and principles of the United Nations, including to maintain international peace and security and the promotion of human rights.' (§ 38).*

Thus, the mere fact that states have decided, for whatever political reason, to mirror existing rules of international law in their policy recommendations cannot free the former of their binding legal force. Otherwise, recommendations such as the one in para 13(f) of the 2015 GGE Report, establishing that a 'State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure', would become a contradiction in terms. As noted by France, Australia, Germany, the United Kingdom, Poland, Brazil and the Dominican Republic, the voluntary, non-binding norms are complementary rather than alternative to existing international law. Thus, compliance with several norms of responsible state behaviour in cyberspace is not only expected on a voluntary basis, but also required as a matter of applicable international law. Where the norms correspond to established rules of international law, the wealth of state practice and attitudes expressed in their implementation (see, e.g. the documents released by the UK, Canada and Australia), serves not only to confirm the applicability of existing rules to ICTs, but also to mould their interpretation as these rules and technologies evolve over time.

Conclusion

Unlike history, international law can be re-written, provided that states agree to new rules by treaty or customary international law. But what has been written or accepted remains there, until such time as new rules have been developed. General rules and principles of international law continue to govern state behaviour, irrespective of the technologies used. For ICTs to be carved out or subjected to new rules, a new treaty or sufficient state practice and opinio juris would be necessary. Yet, not only have states reaffirmed the applicability of extant international law in 'cyberspace', but they continue to act upon it, whether they expressly admit it or not.

1 The Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector

Published 21 May 2020
150 Signatories

We, the undersigned public international lawyers, have watched with growing concern reports of cyber incidents targeting medical facilities around the world, many of which are directly involved in responding to the ongoing COVID-19 pandemic.

We are concerned that the impact of such incidents is exacerbated by the existing vulnerability of the health-care sector to cyber harm. Even in ordinary times, this sector is particularly vulnerable to cyber threats due to its growing digital dependency and attack surface.
We consider it essential that medical facilities around the world function without disruption as they struggle to respond to the COVID-19 pandemic. Any interference with the provision of health-care, including by cyber means, risks further loss of life as thousands continue to die every day.
We support the International Committee of the Red Cross' call on States to protect medical services and medical facilities from harmful cyber operations of any kind.

We emphasize that cyber operations do not occur in a normative void or a law-free zone. As recognized by the United Nations General Assembly, international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful information and communications technology environment.

Guided by these considerations, we agree that the following rules and principles of international law protect medical facilities against harmful cyber operations. We encourage all States to consider these rules and principles when developing national positions as well as in the relevant multilateral processes and deliberations:

1. International law applies to cyber operations by States, including those that target the health-care sector.

2. International law prohibits cyber operations by States that have serious

adverse consequences for essential medical services in other States.

3. International human rights law requires States to respect and to ensure the right to life and the right to health of all persons within their jurisdiction, including through taking measures to prevent third parties from interfering with these rights by cyber means.

4. When a State is or should be aware of a cyber operation that emanates from its territory or infrastructure under its jurisdiction or control, and which will produce adverse consequences for health-care facilities abroad, the State must take all feasible measures to prevent or stop the operation, and to mitigate any harms threatened or generated by the operation.

5. During armed conflict, international humanitarian law requires that medical units, transport and personnel must be respected and protected at all times. Accordingly, parties to armed conflicts: must not disrupt the functioning of health-care facilities through cyber operations; must take all feasible precautions to avoid incidental harm caused by cyber operations, and; must take all feasible measures to facilitate the functioning of health-care facilities and to prevent their being harmed, including by cyber operations.

6. Cyber operations against medical facilities will amount to international crimes, if they fulfil the specific elements of these crimes, including war crimes and crimes against humanity.

7. The application of the aforementioned rules of international law is without prejudice to any and all other applicable rules of international law that provide protections against harmful cyber operations.

'Today's world is marked by rapid technological advances, which present not only unprecedented opportunities but also the risk of significant humanitarian impact. In particular, the use of cyber capabilities for hostile purposes can have devastating consequences for people and societies. In order to address these concerns, we need to urgently clarify the constraints that international law, including international humanitarian law, places on cyber conduct. The Oxford Process has by now become an important platform for the development of such common understandings and I am sure that its outputs will continue to inspire the ongoing international efforts in this area.'

Dr Kubo Mačák, Legal Adviser,
International Committee of the Red Cross

Image credit: Patrick Assalé, Unsplash

Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector

Written by Dapo Akande, Duncan Hollis, Harold Hongju Koh and James O'Brien

First published on EJIL:Talk!, Just Security and Opinio Juris

Many have recently written about the application of international law in cyberspace and to the global COVID-19 pandemic, but relatively few have examined the intersection between these two areas. Notwithstanding that oversight, recent weeks have seen cyberattacks on organizations at the frontline of the response to the COVID-19 pandemic, including malicious cyber operations against the World Health Organization, medical providers, research institutes, pharmaceutical manufacturers, hospitals and hospital networks. In response to these attacks, the European Union issued a statement in which "the European Union and its Member States call[ed] upon every country to exercise due diligence and take appropriate actions against actors conducting such activities from its territory, consistent with international law". Twelve other countries aligned themselves with this declaration. In late March, three authors from the International Committee of the Red Cross (ICRC), writing in their personal capacities, examined the international law protections prohibiting cyberattacks against medical facilities during the pandemic.

These events triggered a two-day virtual workshop at the University of Oxford—co-sponsored by the Oxford Institute for Ethics, Law and Armed Conflict (ELAC) at the Blavatnik School of Government, Microsoft, and the Government of Japan—to discuss these issues. On

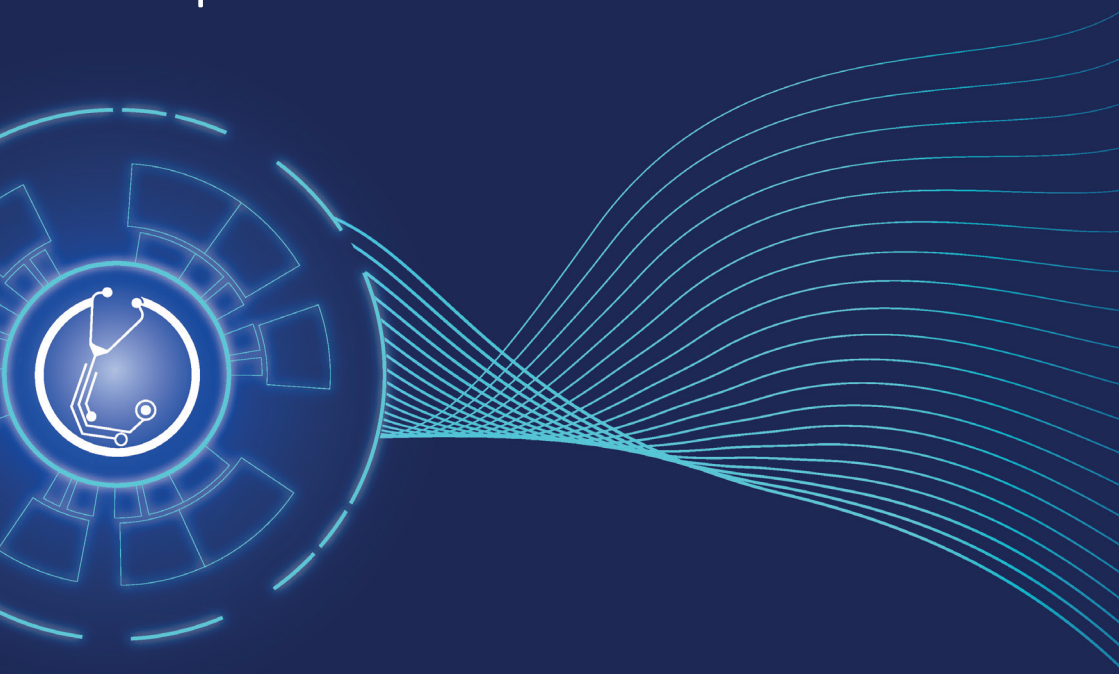
Friday, May 22, 2020, Estonia, as President of the United Nations Security Council, is planning an Arria-Formula meeting of the Council to discuss responsible State behavior in cyberspace, including the international legal protections accorded to healthcare.

Because of the urgency of the current moment, the participants in the Oxford Workshop agreed upon the Oxford Statement below and (here with updated list of signatories), regarding relevant international law rules and principles relating to malicious cyber operations targeting healthcare facilities.The Statement's aim is not to cover all applicable principles of international law, but rather, to articulate a short list of consensus protections that apply under existing international law to cyber operations targeting the health care sector.

The Oxford Statement was opened for signature by international law scholars, and remains open for signature. The Oxford Statement has been transmitted to participants in the May 22, 2020 Security Council meeting in hopes that it will promote discussion and spur clarification of the international law rules in this area.

International law has always been disaster-driven. Deliberate targeting of medical facilities during armed conflict has been called "at once morally indefensible and categorically illegal." The present crisis presents a rare window for making this point of law explicit and unambiguous: in real and virtual space, in times of war and peace. The UN Security Council is finally giving this matter its attention. Global crises create unique opportunities for international lawmaking. International lawyers should not waste this moment.

Virtual workshop
Report



The Oxford Process on International Law Protections in Cyberspace:

Applying International Law in Cyberspace – Protections and Prevention

18 & 19 May 2020

Executive Summary & Key Takeaways

On May 18th and 19th, 2020, the Oxford Institute for Ethics, Law and Armed Conflict (ELAC) held two virtual workshops, sponsored by Microsoft and the Government of Japan, on the topic 'Applying International Law in Cyberspace: Protections and Prevention'. Both workshops were organised around two sessions with identical topics and different participants. The sessions comprised presentations and comments by discussants, followed by open discussions.

The following consensus findings emerged from the discussion:

1. International law applies to cyber operations targeting the healthcare sector.

2. Although a wide range of international law obligations, both positive and negative in character, protect the healthcare sector from harmful cyber operations, these obligations are in need of further specification.

3. International law contains a patchwork of primary obligations with a due diligence standard. These obligations require States to behave in a reasonable way to prevent, halt, mitigate and/ or redress harm. Examples of such obligations include the Corfu Channel and no-harm principles, positive obligations under international human rights law and international humanitarian law.

Summary of Sessions

Welcome and Introductions

The opening remarks given by Professor Dapo Akande and Mr Tomohiro Mikanagi emphasised the timeliness of the workshop. Recent events demonstrated that pandemics and cyber operations need to be analysed in parallel. On the one hand, the previous two months saw a surge in cyberattacks against healthcare facilities engaged in the research of Covid-19 and treatment of patients and thus placed into sharp focus the consequences of such disruptions for the effective response to the pandemic. On the other hand, States have begun to make statements related to the application of international law in the context of cyberattacks against healthcare facilities, thereby fleshing out what responsible behaviour in relation to such facilities ought to be. It is against this background that the two workshops sought to clarify the protective and preventive obligations of States applicable in cyberspace.

Session I

International Law Protections against Malicious Cyber Operations Targeting the Healthcare Sector

Presentation: Dr Kubo Mačák, ICRC

The first presentation, delivered by Kubo Mačák, followed the legal analysis of a background paper prepared with co-authors Laurent Gisel and Tilman Rodenhäuser, which was based on a previous blog post by the authors. The presentation sought to provide an answer to the question: 'what does international law have to say to States when it comes to protection and prevention in the context of cyber operations targeting the healthcare sector?'

To understand the importance of this topic, it is important to realise that the Covid-19 pandemic brought to light both our shared humanity and our shared vulnerability. This vulnerability created by the virus is further exacerbated by our dependence on networks. For instance, the functioning of a hospital can be paralysed by a ransomware attack. Given the risk of loss of life inherent in such attacks, even some cyber

criminals have recently vowed not to target healthcare facilities.

It was emphasised that these cyber operations do not occur in a legal void: international law applies in cyberspace. One of the relevant regimes that were examined was international humanitarian law (IHL), which provides robust legal protection in times of armed conflict. Importantly, IHL applies to all means and methods of warfare and covers cyber operations of belligerent parties. Despite some fears that the applicability of IHL to cyberspace could militarise the domain, such a trend has not been observed, according to Dr Mačák, and IHL in fact places important restrictions on the actions of belligerents. In particular, IHL requires that medical units and personnel be respected and protected at all times. Respect translates into an obligation not to disrupt the facilities and to take all feasible precautions against incidental harm to them. Protection requires that steps be taken to avoid or minimise harm from others. As noted by Dr Mačák, it is hard to conceive of a cyber operation aimed against medical facilities in armed conflict that would somehow be lawful under IHL. Outside of armed conflict, healthcare facilities are protected by other rules of international law, including international human rights law (IHRL). During the presentation, a new norm of responsible State behaviour proposed by the International Committee of the Red Cross was discussed: 'States should not conduct or knowingly support [cyber] activity that would harm medical services or medical facilities, and should take measures to protect medical services from harm.' This norm was seen as reaffirming existing rules of international law.

One strand of criticism against the adoption of this norm takes the view that presenting it as 'new' would suggest the lack of an existing legal framework, or its insufficiency. Another strand of criticism took issue with the focus on the medical context, as this might be seen as suggesting that other critical infrastructure is not similarly protected. The presenter took the view that the addition of a layer of legal protection cannot detract from what the law already provides, that is, that existing protections remain intact and the new norm only serves to fortify the legal protection of medical infrastructure and to

emphasise its vulnerability. As was highlighted by some participants in the open discussion, another potential difficulty with the advancement of a new norm is that there are significant risks of a stalemate in inter-governmental forums if such a new norm is placed on the table.

Discussant: Professor Rain Liivoja, University of Queensland Law School

Rain Liivoja, the discussant on May 18th, emphasised the lack of clarity on the scope of existing rules. For instance, while it is considered that legal protection under IHL extends to data belonging to medical units and personnel, it is unclear whether this would cover electronic medical records stored centrally or shared between healthcare providers. Some participants considered that this protection should extend to all medical records and data, as well as to medical communication. This highlighted the need for a more fine-tuned understanding of e-solutions adopted by States.

Additionally, Professor Liivoja saw the thresholds of the use of force and armed attack as another area of uncertainty. While a lot of attention has been given to the degree of harm to infrastructure, the same cannot be said of the types of injury that may rise to the level of an attack, and in particular injuries that relate to mental health conditions, such as post-traumatic stress disorder.

Finally, he drew attention to the 'legal acrobatics' that some States engage in to avoid the acknowledgment that many cyber operations would infringe the sovereignty of other States or constitute prohibited intervention. One example is the characterisation of targets as belonging to 'essential governmental functions': a qualification used to distinguish between prohibited and non-prohibited conduct. There is, according to Professor Liivoja, a need for further clarification of legal standards and tests in the area.

Discussant: Ms Harriet Moynihan, Chatham House

Harriet Moynihan was the discussant on May 19th, and she addressed in more detail the element of coercion in the prohibition of intervention, the potential thresholds for a violation of this rule, and the question

whether sovereignty exists as a rule or a principle. On coercion, she noted that the element need not be confined to an interpretation that emphasises the dictation of a course of conduct; in fact, the element may be seen as centring on a wrongful deprivation of a State's free will, an act that effectively deprives a State of control over matters of an essentially sovereign nature.

On thresholds in relation to violation of sovereignty, she stressed the need for clear benchmarks in assessing a potential *de minimis* line. These benchmarks would be helpful in order to help delineate where the boundary for a violation lies, particularly in relation to the lower end of interference. This would help inform discussions on whether a range of operations violated international law, including those bearing resemblance to espionage, for instance operations gathering information on the number of patients in a hospital. On sovereignty, Ms Moynihan raised the practical difficulty for States of having a legal obligation by which they are bound, when the substantive contours of that obligation remain unclear.

Open discussion

In the open discussion moderated by Professor Duncan Hollis, the participants raised a number of points related to the scope of existing protections, the elements of the relevant primary rules and the status of norms.

On the prohibition of intervention, some participants questioned whether the element of coercion necessarily implies an action taken to force another State into pursuing, or abstaining from pursuing, a particular line of conduct. It was considered whether coercion could also be interpreted to cover cases where an actor disrupts or inhibits the activities of a State without necessarily advancing any demands. Such action would encroach upon areas in which the State may decide freely, in choices that must remain free ones. An example given was when the target State, as a result of a cyber operation, becomes unable to control its healthcare system. According to other participants, this interpretation of the element of coercion hides the risk of overreach,

as it would extend to the exercise of any jurisdictional power within the State's *domaine réservé*. Others saw difficulties in drawing the line between influence and coercion, and in finding practice supporting the existence of coercion beyond cases involving the use of force.
A related topic that was addressed during the discussion was the existence of a rule of sovereignty separate from the prohibition of intervention. To some, the alternative interpretations of the element of coercion under the non-intervention rule are merely workarounds attempting to circumvent the acknowledgment that a self-standing rule of sovereignty exists. It was noted that States from continental Europe increasingly accept the existence of such a self-standing rule of sovereignty which, unless a State consents otherwise, protects the exercise of governmental powers. Another angle of the discussion on sovereignty centred on the types of intrusion that the rule could cover. In particular, the confidentiality, integrity and availability of systems were seen as pertinent benchmarks to look at, although the precise nature and extent of interference required to reach the level of prohibited conduct remain unclear.

On the choice to focus on specific legal frameworks, some participants opined that the emphasis on IHL, as opposed to IHRL, may incentivise States to resort to cyber warfare, especially when reference is made to the former before an armed conflict takes place. To counter this argument, other participants drew attention to the distinction between regulation and justification. As noted by some commentators, different bodies of law have different strengths: IHL seems to have the strongest restrictions, while peacetime restrictions seem vaguer. Many participants stressed the importance of looking at 'entry points' beyond the discussions on sovereignty and non-intervention. An apposite entry point for peacetime protection was, according to some commentators, IHRL, as there are workable standards for the obligations related to the provision of healthcare. Many commentators shared the sentiment that IHRL has been unjustifiably underemphasised, even though, whether in times of conflict or not, most of the issues discussed in the context of cyber operations against healthcare facilities implicate the duties of States to protect the rights to life and health of those under

their jurisdiction. On the issue of determining the scope of jurisdiction under IHRL, it was agreed that extraterritorial jurisdiction would be the main obstacle to the extension of obligations to third States. One commentator drew the attention to the wealth of regulations of the World Health Organization intersecting with IHRL, and their relevance to the current debates on protection against malicious cyber operations targeting the health sector.

According to some participants, more attention should be paid to certain well-established rules that could cover a broad range of low-level operations, such as the constant care obligation under IHL. Some commentators considered that a focus on IHL and the framework of the resort to force may give rise to heated debates, and, ultimately, an impasse in inter-governmental dialogues that would detract from the careful examination of important peacetime rules, such as the range of due diligence duties.

A question related to the different frameworks applicable in peacetime and in time of armed conflict was that of transitions between regimes. For instance, one participant noted the importance of determining the point of transition between peacetime and armed conflict, and whether such a transition can occur via a cyber operation alone. It was noted that this particular question has been left uncertain in the new ICRC Commentary, and the answer will be fleshed out by the practice and *opinio juris* of States.

Another aspect of the debate focused on the status of norms, such as the Voluntary Norms of Responsible State Behaviour elaborated within the UN Group of Governmental Experts process. While it was acknowledged that such norms can become binding rules, the careful distinction between law and non-law was seen as paramount: only violations of binding rules have legal consequences.

A number of unique features were seen as characterising the discussion, and requiring further elaboration. First, especially for cyber operations against medical facilities, we observe a unique lack of justification for

such acts: the only incentives for them could be ransom, wartime attacks on civilians, desire for general disruption or vandalism. Second, the role and impact of non-State actors have become particularly apparent in the conduct of cyber operations. Unlike conventional conflicts, where the relevance of non-State actors is, in most cases, confined to a regional or local level, in the cyber domain, their power becomes global, and so do the consequences of their attacks. In light of these developments, it was considered that more attention should be paid to the regulation of non-State actors. A third unique facet pertains to the harmful effects of operations, and the foreseeability of results flowing from cyber operations, given the inter-dependence between systems.

Remedies also featured in the discussion, particularly in relation to potential remedies that would directly contribute to the protection of medical facilities. As noted by one participant, if we seek to maximise protection of medical facilities, the concrete remedies that would bolster their protection should be clarified.

Session II

States' Obligations of Due Diligence in Cyberspace

Presentation: Dr Antonio Coco, University of Essex and Dr Talita Dias, University of Oxford

The second session focussed on the types of 'due diligence' standards that exist in binding international legal rules. On May 18th, the session was composed of two presentations, followed by an open discussion. In the second session of May 19th, the first presentation was delivered again, this time with a discussant, and then the session proceeded to an open discussion.

At the beginning of the session, the moderator asked the participants to consider the ways in which ransomware operations may challenge presumptions that operate in the sphere of cyber operations. For instance, while in the past the attacking of particular targets, such as power grids, may have been taken as a strong indicator of attribution to a nation State actor, the contemporary landscape of ransomware

operations shows that such operations can be mounted by non-State actors operating without any political motivation.

The first presentation was based on a paper prepared by Dr Antonio Coco and Dr Talita Dias entitled 'More than Meets the Eye: A Patchwork of Cyber Due Diligence Duties in International Law'.

Starting from the premise that due diligence is a standard of conduct attached to different obligations, the presentation sought to identify the types of primary international rules that contain such a due diligence standard. Some of these rules are part of general international law, such as the 'Corfu Channel' principle and the 'no-harm' principle. Others can be found in specialised branches of international law – for instance positive duties to protect human rights (e.g. the rights to life, health, privacy) under IHRL and positive duties under IHL, like the duty to ensure respect for IHL or the duty to adopt protective precautions against the effects of attacks. In essence, all these rules require States to behave in a reasonable way to prevent, halt, mitigate and/or redress harm. Within this patchwork of due diligence rules, it is still possible to identify strands of commonalities, which can assist in conceptualising the standard itself. For each commonality, however, there are important differences in the contours of each specific primary obligation. For instance, while all due diligence obligations require a nexus between the duty-bearer State and the harm to be acted upon, the specific nexus triggering the obligation of due diligence differs across primary rules. All the various primary obligations only require a State to act when it has (actual or constructive) knowledge of the harm, and the capacity to act (based, for example, on available resources). All the analysed primary rules also share a core obligation to set up a minimal governmental infrastructure which would allow States to exercise due diligence in responding to the harm in question. However, the type and threshold of harm in question, the scope of the measures to be adopted and the legal consequences of a failure to exercise due diligence are rule-specific. Capacity was seen by the presenters as the core of the analysis, featuring both as a trigger and a limit to these duties.

According to the authors of the paper, the debate on whether a standalone rule of cyber due diligence exists misses the point: several duties to behave diligently to prevent, halt and/or redress cyber harms already undoubtedly exist in international law. It was emphasised that international law in its entirety applies to cyberspace by default and that State practice and opinio juris support this reading. Clarity about the various due diligence obligations of States can help maintain a more secure cyber space.

Discussant: Mr Tomohiro Mikanagi, Japanese Ministry of Foreign Affairs

While the first presentation sought to detangle the rules of due diligence and to explore their peculiarities, the second presentation placed the emphasis elsewhere: in the need to find the common elements of all due diligence rules. This presentation was delivered by Mr Tomohiro Mikanagi. Three core elements were identified – seriousness of the harm to be prevented/halted, the capacity to influence perpetrators and the duty to cooperate with other international actors. Capacity to influence was used as a limiting factor: responsibility should be proportionate to a State's capacity to influence. The duty to cooperate was seen as stemming from due diligence, and the relevance of cooperation was emphasised in the 2015 Report of the UN Group of Governmental Experts. In light of these elements, Mr Mikanagi proposed two core principles. The first one postulates that States have the obligation to take measures to prevent and mitigate malicious cyber activities causing serious damage to critical infrastructure or serious violation of human rights in other States proportionate to their capacity to influence potential perpetrators and also to the seriousness of the risk. And turning to cooperation, the second core principle posits that States which have become aware of a serious risk of threat to other States' critical infrastructure and fundamental human rights of the latter's nationals posed by malicious cyber activities emanating from the former's territories have the duty to notify the latter States, and to inquire into such a risk of which the former have become aware. According to Mr Mikanagi, these elements form the basis of due diligence and should be agreed on in order to pursue a meaningful discussion.

Discussant: Professor Heike Krieger, Freie Universität Berlin

Professor Heike Krieger was the discussant of the first presentation on May 19th. She suggested focussing on the no-harm principle, which is not restricted to environmental law and may give the most viable option forward. Its viability can be traced back to its broad sphere of application – to lawful and unlawful behaviour, for acts by States and non-State actors. She agreed that due diligence is a standard, not a rule: the applicable rule would be the no-harm principle, not due diligence as such. Professor Krieger placed an emphasis on procedural obligations, such as the duties to notify, inform, consult, publicly explain, as they are concrete and serve to create trust. During the open discussion, some participants cautioned against an emphasis on notification requirements without carefully investigating their implications. There could be a concern that a duty to notify may in effect require States to reveal their capacities to other States.

Open discussion

In the open discussion moderated by Professor Dapo Akande, some commentators emphasised the need to attach the concept of due diligence to specific primary rules. This is because one cannot say that States are obliged to act diligently in general, they have specific obligations in specific contexts. The term 'due diligence' says nothing on what kind and degree of diligence is due. A fear expressed was that a general discussion of due diligence may dilute our understanding of State obligations: in many cases, States have obligations that require more than diligence, one example being human rights law with its tests of legitimate aims and proportionality.

It was acknowledged by presenters and commentators that many areas remain unclear. For instance, the reference to 'acts contrary to the rights of other States' in the Corfu Channel Judgement of the International Court of Justice remains obscure; the level of control over dispersed data and the exercise of sovereignty over data are still areas in search of answers; the debate on whether the models of extraterritorial jurisdiction for negative and positive obligations differ is still far from settled.

It was noted by a number of participants that the presentations only addressed the 'after' question, i.e. once a State is aware of a malicious cyber operation. A difficult question is raised in the 'before' period – is there an obligation to be aware of specific risks? Taking this to the context of the current pandemic, perhaps a State with few resources in its healthcare sector will have no capacity to monitor what is happening in its cyber environment. The question then is whether it should have been aware, and this is a question that pertains to the factual triggers of such obligations. Deliberate ignorance would not be acceptable.
Still on the level of factual triggers, some participants expressed concern over the impact that these obligations may have on the right to privacy. This question was seen as linking back to the discussion of primary obligations, and of the knowledge standard incorporated in such primary rules. According to one of the presenters, knowledge could be examined in two ways: first, as a procedural obligation to acquire the minimum capacity or infrastructure enabling the State to obtain the necessary information, and second, a due diligence obligation is triggered when there is a foreseeable risk of a forthcoming cyberattack. Any duty to monitor would also depend on capacity. A balance is to be struck when considering potentially conflicting duties of the State, and this balance can be found, for example, in concrete tests, such as those existing under IHRL.

The relationship between due diligence, sovereignty and extraterritorial jurisdiction was also considered. One of the presenters affirmed that all States that have sovereignty have due diligence obligations rooted in the very fact of statehood, as they have a governmental apparatus.
Apart from the specific issues arising out of the need to clarify primary rules containing due diligence standards, the participants discussed the value of engaging in this exercise. Some participants saw the utility of due diligence in that it offers an alternative to the 'attribution' route. Due diligence comes into play when there is a risk to be managed (technical, environmental, coming from another actor) and States are obliged to eliminate or contain that risk.

And while the participants saw the utility of analysing due diligence obligations, some noted the terminological confusion that these standards have provoked. One commentator opined that 'due diligence' in cyberspace has been mainly associated with the Corfu Channel principle. An approach suggested by one participant was to determine whether everyone agrees that the Corfu principle exists under customary law; if so, then the policy debate should be seen as an attempt by some to carve out a rule excluding cyberspace from the principle, rather than as a discussion on whether the rule exists. Finally, the main value of these discussions was seen in the exercise of unpacking what 'reasonableness' in the context of various due diligence standards means, and how States are required to act in specific circumstances. For instance, in the context of extraterritorial jurisdiction under IHRL, reasonableness was seen as an important constraining element: without it, the mere ability of a State to influence something somewhere may be seen as implying that the obligation has been triggered. Additionally, reasonableness plays a role at the stage of determining what measures a State can reasonably be expected to take.

Closing remarks

The closing remarks given by Harold Hongju Koh focussed on the need to turn this time of crisis into a time for international law-making. Clarification of legal standards was considered imperative. There seems to be a sufficient consensus that responsible State behaviour is required, and that this standard of responsible behaviour is mandated by international law. It is at the level of source and content of this rule that silos appear and prevent agreement. This is why it is important to get past these silos, to reach a degree of consensus, and to initiate a process that can build on this first milestone of agreement.

At the end of both workshops, the participants discussed a number of rules and principles that, on May 21st, were made official as the Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector and published on a number of online platforms. The full text of the Statement and the list

of signatories can be found on ELAC's website.

In line with the call for a clarification of legal standards issued in the closing remarks, the Oxford Statement was primarily addressed to, and used by UN member States. Notably, it was mentioned as a good example of how international law applies in cyberspace by the representative of the Dominican Republic, Ambassador, Special Envoy to the Security Council, H.E. Mr. José Singer Weisinger, one of the co-hosts of the UN Security Council Arria-Formula Meeting on Cyber Stability and Responsible State Behaviour in Cyberspace that took place on Friday, 22 May 2020.

List of Workshop Participants

1. Dapo Akande, University of Oxford
2. Meredith Berger, Microsoft
3. Russell Buchan, University of Sheffield
4. Marjolein Busstra, Netherlands Ministry of Foreign Affairs
5. Scott Charney, Microsoft
6. Kaja Ciglic, Microsoft
7. Sarah Cleveland, Columbia University Law School
8. Antonio Coco, University of Essex and University of Oxford
9. Rebecca Crootof, University of Richmond
10. Federica D'Alessandra, University of Oxford
11. Francois Delerue, Institute of Strategic Research of the Military Academy, France
12. Talita Dias, University of Oxford
13. Kristen Eichensehr, UCLA Law School
14. Laurent Gisel, International Committee of the Red Cross
15. Claudio Grossman, American University Washington
16. Duncan B. Hollis, Temple University
17. Zhixiong Huang, Wuhan University
18. Miles Jackson, University of Oxford
19. Tania Jancarkova, NATO Cooperative Cyber Defence Centre of Excellence
20. Eric Jensen, Brigham Young University
21. Kate Jones, University of Oxford
22. Heike Krieger, Freie Universität Berlin
23. Harold Hongju Koh, Yale Law School
24. Masahiro Kurosaki, National Defense Academy of Japan
25. Henning Lahmann, Digital Society Institute, ESMT Berlin
26. Rain Liivoja, University of Queensland
27. Kubo Mačak, University of Exeter and International Committee of the Red Cross
28. Nemanja Malisevic, Microsoft
29. Eviatar Matania, Tel Aviv University
30. Suzuki Masaru, Embassy of Japan in the United Kingdom
31. Tomohiro Mikanagi, Ministry of Foreign Affairs of Japan
32. Tomáš Minárik, National Cyber and Information Security Agency of the Czech

Republic

33. Harriet Moynihan, Chatham House
34. Jan Neutze, Microsoft
35. Georg Nolte, Humboldt University Berlin
36. Jim O'Brien, Albright Stonebridge Group
37. George Papademetriou, Albright Stonebridge Group
38. Patryk Pawlak, European Union Institute for Security Studies
39. Anne Peters, Max Planck Institute for Comparative Public Law
40. Daniela Rakhlina-Powsner, Temple University
41. Tilman Rodenhauser, International Committee of the Red Cross
42. Przemysław Roguski, Jagiellonian University in Kraków
43. Barrie Sander, FGV Direito Rio
44. Michael Schmitt, University of Reading
45. Antonios Tzanakopoulos, University of Oxford
46. Tsvetelina van Benthem, University of Oxford
47. Liis Vihul, Cyber Law International
48. Douglas Wilson, GCHQ
49. Elizabeth Wilmshurst, Chatham House
50. Yuki Yasuda, Ministry of Foreign Affairs of Japan
51. Robert Young, Global Affairs Canada

International law protections against malicious cyber operations targeting the healthcare sector

6 May 2020

This background paper was prepared by Kubo Mačák, Laurent Gisel and Tilman Rodenhäuser, International Committee of the Red Cross (ICRC) Legal Division, on the basis of their article previously published on Just Security.[1] *The views expressed in the document are those of the authors and do not necessarily express institutional positions of the ICRC.*

1 K Mačák, L Gisel and T Rodenhäuser , 'Cyber Attacks against Hospitals and the COVID-19 Pandemic: How Strong are International Law Protections?', Just Security (27 March 2020).

Contents

Introduction

A major hospital in Brno, the Czech Republic's second-biggest city, got hit by a cyber attack on March 13.[1] According to the hospital's management, the attack forced the staff to postpone urgent surgical interventions, reroute new acute patients, and reduce some of their other activities.[2] The hospital is in charge of administering coronavirus tests in the city and the disruption delayed the processing of the tests by several days.[3] Since then, cyber incidents targeting the health-care sector have been reported from countries including France, Spain, Thailand or the United States.[4]

In a situation where most, if not all of us are potential patients, few services are more important than the efficient delivery of health care.

1 S Lyngaas, 'Czech Republic's second-biggest hospital is hit by cyberattack', CyberScoop (13 March 2020).
2 C Cimpanu, 'Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak', ZDNet (13 March 2020).
3 ČTK, 'Výsledky testů na koronavirus zdržel kyberútok na FN Brno' [Coronavirus tests results delayed by cyberattack against University Hospital Brno], České noviny (13 March 2020).
4 A Holmes, 'Hackers are targeting hospitals already stretched thin from fighting the coronavirus — and experts say the worst cyberattacks may be still to come', Business Insider (14 April 2020).

The strain on hospitals around the world is rapidly growing, to which States have responded by mobilizing military medical units,[5] nationalizing private medical facilities,[6] and building emergency hospitals.[7] It is essential that all of these facilities can function without interruption and that they have sufficient resources as they scale up their operations due to the unfolding crisis. However, as noted in a 2019 International Committee of the Red Cross (ICRC) report on the potential human cost of cyber operations, even in ordinary times the health-care sector is particularly vulnerable to cyber attacks due to its increasing digital dependency and 'attack surface'.[8]

In light of the vulnerability of the health-care sector and the threat posed by cyber attacks, a number of States have recently spoken out on the subject. Australia expressed its view that cyber attacks against the health-care sector would go against existing norms on responsible State behavior.[9] Canada condemned such attacks and stressed that States 'must uphold the rules-based international order and the framework of responsible state behaviour in cyberspace'.[10] China stated that 'cyber attacks against institutions fighting the coronavirus pandemic should be condemned around the world'.[11] The Czech Republic and South Korea have suggested that existing norms should be elaborated on to address the protection of the health-care sector.[12] The Netherlands has stated that '[m]alicious cyber operations targeting healthcare systems or facilities could, depending on the specific circumstances, be qualified as

5 S Bradley, 'Swiss militia soldiers get historic call up to fight coronavirus', SWI (17 March 2020).
6 A Payne, 'Spain has nationalized all of its private hospitals as the country goes into coronavirus lockdown', Business Insider (16 March 2020).
7 S Ankel, 'A construction expert broke down how China built an emergency hospital to treat Wuhan coronavirus patients in just 10 days', Business Insider (5 February 2020).
8 ICRC, The Potential Human Cost of Cyber Operations (May 2019) 6.
9 Stilgherrian, 'Australia and US call out cyber attacks on hospitals during COVID-19 pandemic', ZDNet (27 April 2020) ('Australia also considers that the existing norm "States should not intentionally damage critical infrastructure using ICTs" encompasses medical services and facilities.').
10 Canada, Statement on malicious cyber threats to the health sector (30 April 2020).
11 'China: cyber attacks on anti-pandemic institutions should be condemned', Reuters (24 April 2020).
12 Czech Republic, Comments submitted by the Czech Republic in reaction to the initial "pre-draft" report of the Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security (April 2020) at 1; Republic of Korea, Comments on the pre-draft of the OEWG Report (14 April 2020) at para 12.

a violation of international law.'[13] The United Kingdom raised alert that 'attacks by state and non-state actors seeking to undermine the global response to this unprecedented global health crisis endanger lives', while stressing that '[i]nternational law and the norms of responsible state behaviour must be respected'.[14] The United States called such attacks 'deeply irresponsible and dangerous' and at odds with the 'framework of responsible state behavior in cyberspace'.[15] Finally, the EU has 'call[ed] upon every country to exercise due diligence and take appropriate actions against actors conducting such activities from its territory'.[16] While these statements are clear in their disapproval of cyber attacks against the health-care sector, they remain vague on their legal appreciation of such acts.

All of this underlines the urgent need to understand what protections the law offers against such attacks. This paper examines the protections afforded by existing international law. To the extent that rules that govern the behavior of States are discussed, it should be remembered that these apply only if a given operation is attributable to a State (e.g. because it was conducted by a State organ or under the instructions, direction, or control of a State).[17] Experts have already warned of indications that some 'coronavirus-themed cyberattack campaigns' may have been carried out by States.[18] At this stage, however, no such allegation has been made with respect to the Brno hack referred to above.

13 Netherlands, The Kingdom of the Netherlands' response to the pre-draft report of the OEWG (April 2020) at para 18.
14 United Kingdom, 'UK condemns cyber actors seeking to benefit from global coronavirus pandemic' (5 May 2020).
15 United States, Michael R Pompeo, Secretary of State, 'The United States Concerned by Threat of Cyber Attack Against the Czech Republic's Healthcare Sector' (17 April 2020).
16 Council of the EU, 'Declaration by the High Representative Josep Borrell, on behalf of the European Union, on malicious cyber activities exploiting the coronavirus pandemic' (30 April 2020).
17 See International Law Commission, Articles on the Responsibility of States for Internationally Wrongful Acts, UN GA Res 56/83 annex, UN Doc A/RES/56/83 (12 December 2001), Articles 4–11.
18 M Murphy, 'Hospitals under threat as hackers exploit coronavirus to carry out cyber attacks', The Telegraph (17 March 2020) ('Lindsay Kaye from Recorded Future said there are indications that countries including Iran, North Korea, China and Russia are carrying out coronavirus-themed cyberattack campaigns.').

2. Existing rules protecting the health-care sector against cyber attacks

2.1. Individual criminal responsibility

At the individual level, relevant laws protect hospitals – or the health-care sector more generally – from cyber attacks by criminalizing the relevant conduct. This is done primarily within domestic criminal law regimes, which often criminalize conduct that endangers public health and safety, irrespective of the means used. However, international law may also play a role.

In particular, the 65 States[19] that have ratified the 2001 Budapest Cybercrime Convention[20] are bound by international law to criminalize specified cyber activities, such as illegal access,[21] data interference,[22] and system interference.[23] State parties are also obliged to cooperate with each other in investigating and prosecuting acts criminalized by the Convention.[24] Importantly, in 2013, State parties to the Convention expressly agreed that attacks on computer systems essential for the maintenance of public health and safety are covered by the existing provisions of the Convention. [25]

In addition, provided they fulfil the specific requirements of these crimes, certain particularly grave cyber attacks against medical facilities could qualify as international crimes, such as war crimes (see below) or crimes against humanity.[26]

19 Council of Europe, Chart of signatures and ratifications of Treaty 185: Convention on Cybercrime (6 May 2020).
20 Council of Europe, Convention on Cybercrime, ETS No 185 (opened for signature 23 November 2001, entered into force 1 July 2004) (hereafter Budapest Convention).
21 Ibid Article 2.
22 Ibid Article 4
23 Ibid Article 5
24 See ibid Articles 23–35.
25 Council of Europe, Cybercrime Convention Committee, T-CY Guidance Note #6: Critical information infrastructure attacks (5 June 2013) 3.
26 K Ambos, 'International criminal responsibility in cyberspace' in N Tsagourias and R Buchan (eds), Research Handbook on International Law and Cyberspace (Edward Elgar 2015) 141–142.

2.2. International humanitarian law

At the inter-State level, the applicable legal framework depends on the context in which malicious cyber operations occur.

During armed conflicts, international humanitarian law (IHL) provides robust protections for medical services and facilities. This is because one of IHL's fundamental imperatives is 'mitigating, as far as possible, the sufferings inseparable from war'.[27] In war, combatants and civilians may suffer injuries and diseases and they must be tended to. IHL provides the protective framework to diminish their misfortune.

When conflicts and pandemics intersect, these protections are more important than ever: where people whose houses have been destroyed or who have been displaced by conflict live cramped together in shelters and without adequate hygiene facilities, the virus spreads more quickly and widely. But if hospitals are no longer functioning, life-saving treatment will not be available.

Accordingly, IHL requires that medical units, transport and personnel must be respected and protected by the parties to the conflict at all times.[28] In the ICRC's view, basic rules of IHL such as these ones also 'apply in cyberspace and must be respected'.[29] Therefore, belligerents must not harm medical infrastructure through cyber operations and they must take great caution to avoid incidental harm caused by such operations.

In the ICRC's view, this legal protection extends also to the data belonging to medical units and their personnel.[30] Similar views have been

27 Switzerland, Final Record of the Diplomatic Conference of Geneva of 1949 (Federal Political Department 1949) (hereafter Final Record) vol II-A, at 9.
28 See, eg, J-M Henckaerts and L Doswald-Beck (eds), Customary International Humanitarian Law (CUP 2005) (hereafter ICRC CIHL Study) rules 25, 28, and 29.
29 H Durham, 'Cyber operations during armed conflict: 7 essential law and policy questions', ICRC Humanitarian Law & Policy Blog (26 March 2020).
30 ICRC, International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC position paper (November 2019) 8.

expressed by France[31] and by international law experts.[32] Therefore, malicious cyber operations that would impede the functioning of health-care facilities during armed conflict are prohibited by IHL.

Finally, as noted above, a cyber operation may qualify as a war crime provided certain specific conditions are fulfilled.[33] For example, the war crime of directing an attack against a medical facility under the Rome Statute of the International Criminal Court[34] could conceivably be committed using cyber means.

2.3. Use of force, non-intervention, and sovereignty

Paradoxically, the situation is less clear in situations other than armed conflict. There is no standalone international legal rule that would comprehensively protect medical facilities. One has to look to more general rules and principles of international law. Three areas of international law may offer relevant obligations with respect to attacks by a State or its proxies against the health infrastructure of another State: the law on the use of force, the principle of non-intervention, and the principle of sovereignty.

Firstly, international law provides for a general prohibition of the use of force in Article 2(4) of the United Nations Charter. There is consensus among academic commentators that a State-sponsored cyber operation directly resulting in the killing of persons abroad would be covered by this prohibition[35] and some States, like Australia and Estonia, have expressed the view that such cyber operation could amount to a use of force.[36] Such an interpretation would clearly encompass, for

31 France, Ministry of the Armies, 'International Law Applied to Operations in Cyberspace' (9 September 2019) 15.
32 See, eg, MN Schmitt (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (CUP 2017) 515 (hereafter Tallinn Manual 2.0).
33 See generally Ambos (n 26) 121–137.
34 See Rome Statute of the International Criminal Court (opened for signature 17 July 1998, entered into force 1 July 2002) 2187 UNTS 90, Articles 8(2)(b)(xxiv) and (e)(ii).
35 See, eg, Tallinn Manual 2.0 (n 32) 333.
36 See Commonwealth of Australia, Department of Foreign Affairs and Trade, Australia's International Cyber Engagement Strategy (2017), Annex A: Australia's position on how international law applies to State

example, an operation that remotely shuts down ventilators and other life support systems at a big hospital and thereby causes the death of patients. While this prohibition does not cover all cyber attacks against medical facilities, it is critical as it prohibits those attacks that may be expected to have the most serious consequences.

Secondly, international law prohibits all States from intervening in the internal affairs of other States. The United Kingdom, for example, has expressly stated that this prohibition may also cover acts such as the 'targeting of essential medical services'.[37] That still leaves open the question of which medical services are 'essential' – although in the context of the ongoing pandemic, there is little doubt that, for example, a COVID-19 testing facility would so qualify. However, pursuant to the element of coercion, the act in question is prohibited only when designed to compel a targeted State to change its conduct with respect to a matter on which it may otherwise decide freely.[38] Therefore, cyber operations that disrupt medical facilities without being coercive fall outside the scope of the prohibition on interference in the affairs of other States.

Thirdly, cyber operations that interfere with a State's health-care sector could qualify as violations of that State's sovereignty. Sovereignty is traditionally understood as including a State's exclusive right to exercise its functions within its territory.[39] Cyber operations that undermine the provision of health care in another State's territory would appear to interfere with this right. However, this analysis is complicated by the ongoing dispute as to whether there actually is a standalone international legal obligation to respect the sovereignty of other States in cyberspace[40] – or whether sovereignty is 'merely' a principle

conduct in cyberspace, at 90; Estonia, 'President of the Republic at the opening of CyCon 2019' (29 May 2019).

37 United Kingdom, Attorney General Jeremy Wright, 'Cyber and International Law in the 21st Century' (23 May 2018).

38 See ICJ, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v US) (Merits) [1986] ICJ Rep 14 [205]; Tallinn Manual 2.0 (n 32) 317.

39 See Island of Palmas (Netherlands v USA) (Award) (1928) 2 RIAA 829, 838.

40 See, eg, MN Schmitt and L Vihul, 'Respect for Sovereignty in Cyberspace' (2017) 95 Tex L Rev. 1639.

which guides State interactions, but which cannot itself be violated.[41] Under the former view (held by States such as the Czech Republic,[42] France,[43] or the Netherlands[44]), cyber operations that disrupt the functioning of public hospitals abroad would indeed constitute violations of international law.[45] But under the latter view (held by UK[46] and, possibly, the United States[47]), this would not be the case. As noted above, however, the UK at least considers that cyber attacks that target essential medical services may violate the prohibition of intervention.

2.4. International human rights law

It may also be asked whether a State-sponsored cyber operation against the health-care sector of another State could violate international human rights law (IHRL). As 'the same rights that people have offline must also be protected online',[48] States are generally bound by relevant

41 See, eg, GP Corn and R Taylor, 'Sovereignty in the Age of Cyber' (2017) 111 AJIL Unbound 207.
42 Czech Republic, Statement by Mr. Richard Kadlčák, Special Envoy for Cyberspace, 2nd substantive session of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (11 February 2020) ('[t]he Czech Republic concurs with those considering the principle of sovereignty as an independent right and the respect to sovereignty as an independent obligation').
43 France, Ministry of the Armies, 'International Law Applied to Operations in Cyberspace' (9 September 2019) 6 ('Any unauthorised penetration by a State of French systems or any production of effects on French territory via a digital vector may constitute, at the least, a breach of sovereignty').
44 Netherlands, Ministry of Foreign Affairs, 'Letter to the parliament on the international legal order in cyberspace' (5 July 2019) 2 ('countries may not conduct cyber operations that violate the sovereignty of another country').
45 See also T Mikanagi and K Mačák, 'Attribution of cyber operations: an international law perspective on the Park Jin Hyok case', (2020) 9 Cambridge Journal of International Law 51, 73 (arguing that prompt and efficient patient care is a critical government service, the denial of which would likely be perceived by States as unlawful).
46 United Kingdom, Attorney General Jeremy Wright, 'Cyber and International Law in the 21st Century' (23 May 2018) (stating that he was 'not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government's position is therefore that there is no such rule as a matter of current international law').
47 United States, DOD General Counsel Remarks at U.S. Cyber Command Legal Conference (2 March 2020) ('The implications of sovereignty for cyberspace are complex, and we continue to study this issue and how State practice evolves in this area, even if it does not appear that there exists a rule that all infringements on sovereignty in cyberspace necessarily involve violations of international law.') (emphasis added).
48 UN Human Rights Council, Resolution 32/13 (The promotion, protection and enjoyment of human rights on the Internet), UN Doc A/HRC/RES/32/13 (18 July 2016), para 1.

obligations – such as those derived from the right to health enshrined in Article 12 of the International Covenant on Economic, Social and Cultural Rights (ICESCR) or the right to life enshrined in Article 6 of the International Covenant on Civil and Political Rights (ICCPR).

Today, it is widely – though not universally – accepted that these IHRL treaties bind States with respect to all individuals subject to their jurisdiction, whether these persons find themselves inside or outside a given State's territory.[49] While domestic application of IHRL is well understood, questions remain with respect to the precise extraterritorial reach of the relevant IHRL obligations.

According to the UN Human Rights Committee's General Comment 31, States owe the obligations under the ICCPR to all persons within their 'power or effective control'.[50] However, different views exist on whether individuals affected by cyber operations abroad are under the acting State's power or effective control.

On the one hand, some argue that this would only be the case if the State exercised effective control over the territory in which the operation is conducted, or had physical control over the victims.[51] On this view, cyber interference with a medical facility on foreign territory would normally be outside of the scope of the acting State's obligations under IHRL.

49 See ICJ, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion) [2004] ICJ Rep 136 [111] (ICCPR) and [112] (ICESCR); UN Human Rights Committee, General Comment No. 31 (The Nature of the General Legal Obligation Imposed on States Parties to the Covenant) UN Doc CCPR/C/21/Rev.1/Add. 13 (26 May 2004), para 10 ('a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party'); UN Committee on Economic, Social and Cultural Rights, General comment No. 24 (State obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities), UN Doc E/C.12/GC/24 (10 August 2017), para 27 ('extraterritorial obligations of States under the Covenant follow from the fact that the obligations of the Covenant are expressed without any restriction linked to territory or jurisdiction'); but see, eg, UN Human Rights Committee, Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding observations of the Human Rights Committee: United States of America, UN Doc CCPR/C/USA/CO/3/Rev.1 (18 December 2006), para 10 (noting the US position 'that the Covenant does not apply with respect to individuals under its jurisdiction but outside its territory').

50 UN Human Rights Committee, General Comment No. 31 (The Nature of the General Legal Obligation Imposed on States Parties to the Covenant), para. 10.

51 See Tallinn Manual 2.0 (n 32) 185, para 9.

On the other hand, others take the view that if a State's action can restrict an individual's ability to exercise or enjoy a human right, then that State is in power or effective control over the individual with respect to that right.[52] Without specifically referring to cyber operations, human rights treaty bodies have expressed themselves in ways that would support such a broader interpretation. With regard to the right to health, the UN Committee on Economic, Social, and Cultural Rights has argued that 'States parties have to respect the enjoyment of the right to health in other countries'.[53] With regard to the right to life, the UN Human Rights Committee opined recently that a State's obligations to respect and to ensure this right extend to 'persons located outside any territory effectively controlled by the State, whose right to life is nonetheless impacted by its military or other activities in a direct and reasonably foreseeable manner'.[54] This could be the case, for example, if a cyber operation interfered with ventilators providing life support for COVID-19 patients in intensive care units.

In other words, there are diverging views on the scope of the applicability of IHRL generally, and accordingly, on the extent of the protection that IHRL affords to medical facilities specifically, against cyber operations.

By contrast, it is less controversial that States parties to the ICESCR have the obligation to respect, protect, and fulfil the right to health of all persons under their jurisdiction. The Committee on Economic, Social, and Cultural Rights has argued that the obligation to protect the right to health requires 'States to take measures that prevent third parties from interfering with [the right to health under] article 12'.[55] While the Committee has not pronounced itself on cyber-specific measures,

52 See Tallinn Manual 2.0 (n 32) 185, para 10.
53 UN Committee on Economic, Social and Cultural Rights, General Comment No. 14 (The right to the highest attainable standard of health) UN Doc E/C.12/2000/4 (11 August 2000), para 39.
54 UN Human Rights Committee, General Comment No. 36 (On article 6 of the International Covenant on Civil and Political Rights, on the right to life) UN Doc CCPR/C/GC/36 (30 October 2018), para 63.
55 UN Committee on Economic, Social and Cultural Rights, General Comment No. 14 (The right to the highest attainable standard of health) UN Doc E/C.12/2000/4 (11 August 2000), para 33.

it may be expected that States would at least have 'to regulate the activities of individuals, groups or corporations so as to prevent them from violating the right to health of others',[56] and to take measures to enforce such regulations.[57]

3. New norm against cyber attacks on medical facilities and services

The above analysis demonstrates that various bodies of international law afford strong protections to medical facilities against cyber operations. Depending on how international law is interpreted, it could be deemed to prohibit any hostile cyber operation against medical services – though certain interpretations may leave some loopholes. This is a matter of concern considering the importance of medical services for every one of us.

In this regard, the ICRC recently proposed for the consideration of States participating in the United Nations Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG), a new norm of responsible State behavior in cyberspace.[58] This norm would require that 'States should not conduct or knowingly support [cyber] activity that would harm medical services or medical facilities, and should take measures to protect medical services from harm.'[59] It would reaffirm existing prohibitions under international law applicable during both armed conflict and peacetime – or, depending on the view one takes on peacetime law, strengthen it.

It is sometimes said that in the midst of every crisis lie opportunities. This time is no different. The current global pandemic is highlighting

56 Ibid, para 51.
57 Ibid, para 49 ('Violations of the right to health can also occur through the … the failure to enforce relevant laws.').
58 ICRC, Norms for responsible State behavior on cyber operations should build on international law: Statement to the UN Open-ended working group on developments in the field of information and telecommunications in the context of international security; Second substantive session; Agenda item "Norms, rules and principles" (11 February 2020).
59 Ibid.

the absolutely essential importance of a well-functioning public health-sector. We hope that this crisis will create the necessary impetus for the international community to affirm, in an unequivocal manner, that international law comprehensively prohibits cyber operations against medical services not only in times of war, but at all times.

Suggested points for discussion

1. What protections does international law offer against malicious cyber operations targeting the healthcare sector?

2. To what extent do existing IHL protections for medical facilities and medical services apply in the cyber context? Is it adequate and sufficient considering the specific characteristics of cyberspace or are there any gaps in the protection offered by existing IHL rules?

3. Under what circumstances could a cyber operation against a medical facility or medical service amount to a use of force under Article 2(4) of the UN Charter?

4. Does targeting essential medical services violate the prohibition of non-intervention irrespective of whether it is coupled with an attempt to coerce the target State?

5 Does the interpretation of sovereignty as a rule mean that all peacetime malicious cyber operations against the health-care sector are unlawful under international law, as long as these operations are attributable to States? Could the interpretation of sovereignty as a principle also be understood as compatible with the view that all such operations are forbidden?

6. Do States have an international law obligation to take measures to prevent their cyber infrastructure from being used for cyber operations against medical facilities abroad?

7. Does endangering the health of individuals abroad through cyber means, if attributable to a State, interfere with those individuals' right to life or right to health under IHRL?

8. Does the norm proposed by the ICRC strengthen or weaken the existing international law framework?

9. What responses are available under international law to the State on whose territory the targeted medical facility is based?

10. What types of cyber operations against medical facilities or medical services may qualify as international crimes?

Cyber Due Diligence: A Patchwork of Protective Obligations in International Law

Antonio Coco and Talita Dias

Abstract

With a long history in international law, the concept of due diligence has recently gained traction in the cyber domain. It features as a promising avenue to hold States accountable for harmful cyber operations originating from or transiting through their territory, in the absence of attribution. Despite this renewed interest, much confusion surrounds its nature, content and scope. Particularly, it remains unclear whether due diligence is a general principle of international law, a self-standing obligation or a standard of conduct, and whether there is a specific rule requiring diligent behaviour in cyberspace. We seek to clarify those questions by revisiting existing cases and studies and surveying recent State practice and opinio juris. We suggest that, whether or not there is a general principle of due diligence or a standalone rule of 'cyber due diligence', the expression is at the very least a shorthand for a patchwork of different obligations applying to cyberspace and other domains. At their core is a flexible standard of reasonable care requiring States to prevent, halt and/or redress a range of online harms. But before they can be bundled together by reason of this and other similarities, these obligations ought to be disentangled and unpacked.

1. Introduction

Due diligence has become a buzz word in the cyber domain in recent years. The renewed interest in the concept can be explained by the persistent challenges of factually and legally attributing malicious cyber operations to States. Anonymising and rerouting techniques, such as VPNs and other IP (Internet Protocol) spoofing software have compounded the attribution problem.[1] In this context, due diligence

1 Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm', 21 Journal

features as a promising route to increase peace, security and stability in cyberspace by requiring States to do their best to prevent, halt and/or remedy a range of known or foreseeable cyber harms emanating from or transiting through their territory, regardless of who or what caused them. For instance, during the COVID-19 pandemic, EU member States have 'call[ed] upon every country to exercise due diligence and take appropriate actions against actors conducting [malicious cyber operations] from its territory, consistent with international law'.[2]

Yet controversy remains as to whether States are bound by an obligation to behave diligently in cyberspace, a domain that comprises information and communication technologies (ICTs) having a physical, logical and personal dimension.[3] On the one hand, the 2015 report by the United Nations (UN) Group of Governmental Experts (GGE) on cybersecurity, adopted by consensus by the UN General Assembly,[4]

---

of Conflict & Security Law (JCSL) (2016) 429, at 432.

2 Council of the European Union (EU), Press Release: 'Declaration by the High Representative Josep Borrell, on behalf of the European Union, on malicious cyber activities exploiting the coronavirus pandemic' (2020), available at https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/. A similar Statement was made by the EU and endorsed by member States during the UN Security Council Arria-Formula Meeting on Cyber stability and conflict prevention: see Statement on behalf of the European Union by Mr. Pawel HERCZYNSKI, Managing Director for CSDP and Crisis Response, European External Action Service (2020), available at https://vm.ee/sites/default/files/Estonia_for_UN/20_05_22_arria_cyber_eu_Statement_as_delivered_unread_paras.pdf, at 2; and, e.g., Joint Statement from Denmark, Finland, Iceland, Sweden and Norway by Ambassador Mona Juul at the Arria-meeting on Cyber stability and conflict prevention (2020), available at https://www.norway.no/en/missions/UN/Statements/security-council/2020/arria-cyber-stability-and-conflict-prevention. Along the same lines, but without explicitly mentioning due diligence, see Republic of Poland, Statement by H.E. Tadeusz Chomicki Ambassador for Cyber & Tech Affairs Ministry of Foreign Affairs (2020), available at https://vm.ee/sites/default/files/Estonia_for_UN/Statement_of_poland_arria_un_sc_on_cyber_22.05.2020.pdf, CAPACITY BUILDING (2020), available at https://vm.ee/sites/default/files/Estonia_for_UN/riunione_del_cds_in_formato_arria.pdf, at 1. It is also worth noting that over a hundred and thirty scholars and practitioners acting in their individual capacity accepted that States already have obligations to prevent malicious cyber operations emanating from their territory or jurisdiction against the healthcare sector, especially during the COVID-19 outbreak: see The Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector (2020), available at https://elac.web.ox.ac.uk/the-oxford-Statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea.

3 437, at 454, fn 88. See also Tsagourias, 'The Legal Status of Cyberspace', in N. Tsagourias and R. Buchan (eds.), Research Handbook on International Law and Cyberspace (2015) 13. See also Johnson, Post, 'Law and Borders: The Rise of Law in Cyberspace', 48 Stanford Law Review (1996) 1367.

4 GA Res. 70/273, 30 December 2015, § 1-2(a).

indicates that States 'should not knowingly allow their territory to be used for internationally wrongful acts using ICTs [information and communication technologies].[5] The provision is explicitly framed as a 'voluntary, non-binding norm' of responsible State behaviour in cyberspace. On the other hand, the group of experts involved in the second edition of the Tallinn Manual on the International Law Applicable to Cyber Operations agreed that a general rule or principle of this kind already exists in customary international law, and is applicable in cyberspace.[6] According to Rule 6 of the Manual, such rule requires a State to 'exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other states.'[7] Neither of these views has gone unchallenged.[8]

We contend that it is not accurate to frame the current debate surrounding the application of due diligence to cyberspace in 'all-or-nothing' terms. The debate seems to imply that either consensus has been reached on the existence and application of such a general principle or rule to ICTs, or there would be a legal gap: States would have no obligation whatsoever to prevent, halt or redress harmful cyber operations emanating from or transiting through their territory. We submit that such framing misses the point, and that the concept of 'cyber due diligence' actually brings more to the table than is often assumed. Whether or not a general principle of due diligence applies to

5 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE), UN Doc. A/70/174, 22 July 2015 ('UN GGE Report 2015'), § 13(c).

6 M. Schmitt (ed.), Tallinn Manual 2.0 (2017), at 30, Rule 6, and at 43, Rule 7.

7 M. Ibid., at 30. The Manual is the result of the work of a group of experts, which purports to comprehensively analyse how international law applies in cyberspace.

8 For instance, Jensen and Watts are cautious about legal basis of this rule, recognizing its advantages but also warning about its drawbacks. See Jensen and Watts, 'A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?', 95 Texas Law Review (2017) 1555, at 1568–1575. With respect to the supposed burden that the UN GGE Recommendation would impose on States, making them wary to accept it, see L. Adamson, 'Recommendation 13(c)', in United Nations Office of Disarmament Affairs, Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary (2017) 49, at 55, § 12.

ICTs or a single, cyber-specific version of this obligation exists, States continue at the very least to be bound by a patchwork of due diligence duties or 'protective obligations' applying by default to cyberspace. These are found in several rules of international law requiring States to prevent, halt and/or redress a variety of harms, online and offline.

Although great confusion surrounds its exact meaning and scope, the concept of due diligence has a long history and pedigree in international law. It has been recognized implicitly or explicitly in a series of landmark cases before international courts and tribunals, such as *Corfu Channel*,[9] *Island of Palmas*,[10] *Nicaragua*,[11] *Pulp Mills*[12] and *Bosnian Genocide*[13]. Obligations to exercise (or act with) due diligence exist in general international law as well as several specialised regimes, including international environmental law, law of the sea, diplomatic protection, international investment law, international humanitarian law and international human rights law, under treaty or customary international law.[14] For instance, they feature in treaties dealing with transnational criminal cooperation[15] and deep seabed mining. [16]

This paper begins by clarifying the meaning and status of the concept of due diligence in general international law (Section 2). Section 3, then, explains why the entirety of international law — including duties of due

9 Corfu Channel Case (United Kingdom v Albania), Judgment, 9 April 1949, ICJ Reports (1949) 4, at 22.
10 Island of Palmas Case (or Miangas), United States v Netherlands, Award, 4 April 1928, II RIAA 829 (1928), ICGJ 392 (PCA 1928), at 839.
11 Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America), Judgment, 27 June 1986, ICJ Reports (1987) 14, para 157.
12 Pulp Mills on the River Uruguay, Case Concerning (Argentina v Uruguay), Judgment, 20 April 2010, ICJ Reports (2010) 14, paras 101, 187, 197, 204, 223.
13 Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro), Judgment, 26 February 2007, ICJ Reports (2007) 43, paras 430-431.
14 Koivurova, 'Due Diligence', Max Planck Encyclopaedia of Public International Law (MPEPIL) (2010), available at opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1034?prd=EPIL, paras 29-31, 45.
15 E.g., Article 18, International Convention for the Suppression of the Financing of Terrorism, 1999, 2178 UNTS 197; Article 7, United Nations Convention against Transnational Organized Crime, 2000, 2225 UNTS 209.
16 Articles 139, 153(4) and Annex III, Article 4(4), Convention on the Law of the Sea, 1982, 1833 UNTS 397; Responsibilities and obligations of States with respect to activities in the Area, Advisory Opinion, 1 February 2011, ITLOS Reports (2011) 10, paras 107-123, 136, 141-142, 147, 189, 217, 219, 239.

diligence — applies by default to cyberspace, in the absence of a rule to the contrary. This claim is backed by evidence of relevant State practice and expressions of opinio juris. Subsequently, in what is this paper's main contribution to the current academic debate, Section 4 maps out four sets of due diligence or protective duties applying to cyberspace. Two of these can be traced to primary obligations of general applicability in international law: a) the duty of States not to knowingly allow their territory to be used for acts that are contrary to the rights of third States, which we call the 'Corfu Channel principle';[17] b) States' duty to prevent and remedy significant transboundary harm, even if caused by lawful activities, known as the 'no-harm' principle. In addition, specific bodies of international law establish due diligence duties which also apply to cyberspace. Of particular relevance to ICTs are c) the obligation of States to protect human rights within to their jurisdiction; and d) States' duties to ensure respect for international humanitarian law and to adopt precautionary measures against the effects of attacks in the event of an armed conflict. We locate the legal basis of each of those primary rules in customary or conventional international law and unpack the various standards of due diligence which they require from States in cyberspace. Lastly, Section 5 demonstrates that, despite the concept's multifaceted nature, common features underlie cyber due diligence duties in international law.

Our findings seem to point to one overarching conclusion: although not a silver bullet against all cybersecurity challenges, this comprehensive international legal 'patchwork' of due diligence duties has a central place in the pursuit of a more secure cyberspace.

17 Reinisch and Beham frame it as a 'conflict-related no harm rule', in 'Mitigating Risks: Inter-State Due Diligence Obligations in Case of Harmful Cyber-Incidents and Malicious Cyber-Activity – Obligations of the Transit State', 58 German Yearbook of International Law (GYIL) (2015) 101, at 106.

2. The Nature and Function of Due Diligence in International Law

Despite the renewed interest in due diligence,[18] the concept is not new. It has been variously and often inconsistently described as a general principle of law, one or more self-standing State obligation(s) of conduct, or a standard of behaviour applying in different areas of international law.[19] The modern origins of the concept can be traced to a series of nineteenth and early twentieth century arbitrations relating to the protection of aliens abroad.[20] Already at that time, due diligence was linked to a positive obligation of conduct, a 'best efforts' duty, requiring States to act with reasonable care in the circumstances, and holding them responsible for wilfully negligent omissions. Later on, the *Island of Palmas* arbitral award found that due diligence is a corollary of States' sovereign rights over their territory requiring them to protect the rights of other States therein.[21] Since then, the concept has evolved into different primary rules of international law, with different elements and scopes of application.

First, in the *Corfu Channel* case, the International Court of Justice (ICJ) held that 'it is every State's obligation not to allow knowingly its territory to be used for *acts contrary to the rights of other States*,'[22] most — but not all — of which constitute internationally wrongful acts.[23] This duty, framed as a 'well-recognized principle of international law', applies generally to all States,[24] and a failure to exercise the requisite degree of

18 For general studies on the topic see, e.g., International Law Association (ILA), Study Group on Due Diligence, 2nd Report (2016), available at https://www.ila-hq.org/index.php/study-groups; Koivurova, supra note 14; H. Krieger, A. Peters and L. Kreuzer (eds.), Due Diligence and Structural Change in the International Legal Order (forthcoming, 2020); J. Kulesza, Due Diligence in International Law (2016); Pisillo-Mazzeschi, 'The Due Diligence Rule and the Nature of the International Responsibility of States', 35 GYIL (1992) 9.

19 See McDonald, 'The Role of Due Diligence in International Law', 68 International and Comparative Quarterly (ICLQ) (2019) 1041, at 1043–1044, fn 13; Koivurova, supra note 14, paras 1-2 (referring to due diligence as 'an obligation of conduct' as well as a 'concept' and a 'general principle of law').

20 See, e.g., Alabama Claims Arbitration (USA v UK) (1872) 29 RIAA 125, at 127, 129, 131-132; Wipperman Case (USA v Venezuela) (1887), reprinted in John Bassett Moore, History and Digest of the International Arbitrations to Which the United States Has Been a Party, vol. 3 (1898–1906), at 3041; Neer Case (USA v Mexico) (1926) 4 RIAA 60, at 61-62.

21 Island of Palmas, supra note 10, at 839.

22 Emphasis added. Corfu Channel, supra note 9, at 22.

23 See Section 4.A, below.

24 Corfu Channel, supra note 9, at 22.

diligence gives rise to State responsibility.[25]

Second, as a result of the growing concern over environmental and other hazards crossing national borders, due diligence also features in the general obligation not to cause significant transboundary harm to territory, persons or property.[26] As early as 1941, the Trail Smelter arbitral tribunal found that a State 'owes at all times a duty to protect other states against injurious acts by individuals from within their jurisdiction.'[27] Likewise, Article 3 of the International Law Commission (ILC)'s 2001 Draft Articles on Prevention of Transboundary Harm from Hazardous Activities,[28] recognises a duty of States to 'take all appropriate measures to prevent significant transboundary harm or at any event to minimize the risk thereof'. This provision mirrors customary international law[29] and is, according to the ILC, an 'obligation of due diligence', requiring States not to successfully prevent or halt significant transboundary harm, but 'to exert [their] best possible efforts to minimize [such] risk'. The customary basis of this duty, known as the 'no-harm' or 'good neighbourliness' principle, has also been affirmed by the ICJ,[30] which noted its origins in the broader 'principle of prevention', along with the Corfu Channel dictum.[31] However, the no-harm principle is not limited to acts contrary to the rights of other States, but requires States to prevent any significant transboundary harm, even if caused by *lawful* activities.[32] Moreover, a breach of the no-harm principle gives rise to liability to redress the harm,[33] with State

25 See Article 14(3), International Law Commission (ILC), Articles on Responsibility of States for Internationally Wrongful Acts, GA Res. 56/83, 12 December 2000 (ARSIWA).
26 See ILC, Draft articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries, in Report of the International Law Commission on the work of its fifty-third session (23 April–1 June and 2 July–10 August 2001), UN Doc. A/56/10, 144, at 148-149. See also Brunée and Meshel, 'Teaching an Old Law New Tricks: International Environmental Law Lessons for Cyberspace Governance', 58 GYIL (2015) 129, at 134–135; Koivurova, supra note 14, paras 16, 23, 44-45.
27 Trail Smelter Case (USA v Canada) (1941) 3 RIAA 1911, at 1963.
28 ILC, Draft Articles on Prevention, supra note 26.
29 Koivurova, supra note 14, para 10.
30 Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 8 July 1996, ICJ Reports (1996) 226, para 2.
31 Pulp Mills, supra note 12, para 101.
32 ILC, Draft Articles on Prevention, supra note 26, at 150.
33 Ibid.

responsibility arising subsequently from a failure to redress it. [34]

Similar duties to behave diligently exist under international human rights law (IHRL). These are positive obligations of States to protect and ensure individual human rights, whether online or offline,[35] to the extent possible.[36] Likewise, the duties to ensure respect for international humanitarian law (IHL) and to take precautions to protect civilians against the effects of attacks during armed conflict are also due diligence obligations.[37] And other more or less specific duties of reasonable care arise in respect of different harms, such as the duty to prevent genocide under Article I of the Genocide Convention,[38] the customary duty to protect aliens and the obligation to prevent marine pollution under Article 194(2) of the UN Convention on the Law of the Sea.[39]

This variety of primary rules recognising a duty of reasonable care suggests that 'due diligence' is better framed as a standard of behaviour which makes up different State obligations and varies across different fields, duty-bearers and factual circumstances.[40] Thus, references to 'due diligence obligations' or 'duties of due diligence' in international law are simply a shorthand for a series of obligations which have in common the imposition of a due diligence standard.[41] In a way, breaches of due diligence come close to the concept of negligence, found in many domestic legal systems.[42] As the International Law Association (ILA) found in its recent study on the topic:

34 Walton, 'Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law', Yale Law Journal (2016) 1460, at 1502.
35 See also UN Human Rights Council (HRC), Res. 32/13 ('The promotion, protection and enjoyment of human rights on the Internet'), UN Doc. A/HRC/RES/32/13, 1 July 2016, § 1.
36 See generally Koivurova, supra note 14, para 45.
37 Ibid., para 31.
38 Convention on the Prevention and Punishment of the Crime of Genocide, 1948, 78 UNTS 277. See also Bosnian Genocide, supra note 13, paras 430-431.
39 Supra note 16.
40 See Krieger and Peters, 'Due Diligence and Structural Change in the International Legal Order', in Krieger, Peters and Kreuzer, supra note 18. See also McDonald, supra note 19.
41 See Koivurova, supra note 14, paras 8-9.
42 Kolb, 'Reflections on Due Diligence Duties and Cyberspace', 58 GYIL (2015) 113, at 116; Jensen and Watts, supra note 8, at 1566; Pisillo-Mazzeschi, supra note 18, at 40, 42; Neer case, supra note 20, at 61.

> *'At its heart, due diligence is concerned with supplying a standard of care against which fault can be assessed. It is a standard of reasonableness, of reasonable care, that seeks to take account of the consequences of wrongful conduct and the extent to which such consequences could feasibly have been avoided by the State or international organisation that either commissioned the relevant act or which omitted to prevent its occurrence.'* [43]

Those various 'due diligence duties' all seem to involve a triangular relationship between: a) the duty-bearer, i.e. the State having an obligation to behave diligently in preventing, halting or redressing the harm or the risk thereof; b) the harm's source, i.e. the State, non-State entity or natural event causing the harm; c) the beneficiary of the duty, i.e. the State or non-State entity suffering the consequences of the harm.[44] As such, due diligence duties have been commonly associated with the idea that States must prevent, stop or redress a variety of harms or risks to persons, property or territory, ranging from internationally wrongful acts to lawful activities or even accidents. Each primary obligation to exercise due diligence is triggered and limited by a variety of factors, including: a) the existence of a specific type of harm or risk; b) the crossing of a threshold of seriousness of this harm or risk; c) a nexus between the State and the harm or risk in question, d) some degree of knowledge of the harm or risk and e) a State's capacity to act in the circumstances.[45] However, as will become clearer in the following sections, each of those elements might differ across various due diligence duties.

We contend that several duties of due diligence found in different branches of conventional and customary international law cover numerous aspects, uses and consequences of ICTs, as they do with other domains or technologies. In what follows, we first establish the applicability of some of those duties in cyberspace. We then delve deeper into the extent to which these duties require States to prevent, halt or redress harmful cyber operations or online harms.

43 Emphasis added. ILA Study, supra note 18, at 2. See also Kulesza, supra note 18, at 262-270.
44 Besson, 'Due Diligence and Extraterritorial Human Rights Obligations – Mind the Gap!', 9:1 ESIL Reflections (2020) 2, at 4-5.
45 See Section 4 below.

3. The Applicability of Existing Due Diligence Duties in Cyberspace

As a preliminary point, the applicability of existing due diligence obligations to cyberspace might be challenged on two legal bases. First, one may query whether certain international obligations conceived for the 'offline' world equally apply to cyberspace, as a new domain or technology.[46] Secondly, one may wonder whether States have, in their practice and expressions of opinio juris, actively carved out cyberspace from the scope of application of said duties.

In addressing those possible objections, it is important to note that States and international institutions have consistently affirmed the application of international law as a whole to cyberspace, including, in particular, rules and principles that flow from sovereignty.[47] And this is

46 See, mutatis mutatis, Corn and Taylor, 'Sovereignty in the Age of Cyber', 111 AJIL Unbound (2017) 207, at 208 (challenging on a similar basis the applicability of a rule of sovereignty to cyberspace). See also Note Of. 4VM.200-2019/GJL/lr/bm, from Mr. Gabriel Juárez Lucas, Fourth Vice Minister of the Interior Ministry of the Republic of Guatemala to Luis Toro Utillano, Technical Secretariat, Inter-American Juridical Committee, June 14, 2019, cited in Organization of American States (OAS), Improving Transparency — International Law and State Cyber Operations: Fourth Report (Presented by Prof. Duncan B. Hollis), OEA/Ser.Q, CJI/doc. 603/20 rev.1, 5 March 2020, § 21 (expressing support for the application of international law to cyberspace but noting that there could be areas where 'the novelty of cyberspace does preclude the application of certain international rights or obligations.').

47 See, e.g., Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/68/98, 24 June 2013 ('UN GGE Report 2013'), § 19; UN GGE Report 2015, supra note 5, §§ 24-28; United States (US) Department of Defense, General Counsel Remarks at US Cyber Command Legal Conference, Remarks By Hon. Paul C. Ney, Jr. (2020), available at https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference; US Government, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (2011), available at https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, at 9; Australian Department of Foreign Affairs and Trade (DFAT), Australia's Non Paper: 'Case studies on the application of international law in cyberspace' (2020), available at https://www.dfat.gov.au/sites/default/files/australias-oewg-non-paper-case-studies-on-the-application-of-international-law-in-cyberspace.pdf, at 4, 7-11; Cyber and International Law in the 21st Century, Speech by United Kingdom Attorney General Jeremy Wright QC MP (2018), available at https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century, at 3-6; France, Ministry of Defence, Droit International Appliqué Aux Opérations Dans Le Cyberespace (2019), available at https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqu%C3%A9+aux+op%C3%A9rations+Cyberespace.pdf at 6-17; Keynote address by the Minister of Defence of the Kingdom of the Netherlands, Ms. Ank Bijleveld (2018), available at https://english.defensie.nl/downloads/speeches/2018/06/21/keynote-address-by-the-minister-of-defence-ms.-ank-bijleveld-marking-the-first-anniversary-of-the-tallinn-manual-2.0-on-the-20th-of-june-2018. More recent expressions of this view include: Comments submitted by the Czech Republic in reaction to the initial "pre-draft" report of the Open-Ended Working Group on developments in the field of information and

because rules of general international law apply, by default and across the board, to all areas of State activity. This is so to the extent that the activities in question fall within the scope of those rules, and exceptions or more specific rules do not apply.[48] For this reason, several States have stressed that rules of international law are technology-neutral, even if questions might arise as to how they apply to new means of communication.[49] After all, as a means to a variety of ends, cyberspace or ICTs cannot be severed from the activities to which they serve and, consequently, from the rules governing them.

Two keys rules deriving from the principle of sovereignty and applying generally in international law are precisely the Corfu Channel and the no-harm principles. Thus, the presumption we ought to proceed from is that they apply to ICTs, in the absence of *leges speciales* to the contrary.[50] In the same vein, the scope of application of IHRL and IHL

telecommunications in the context of international security (2020), at 2; The Kingdom of the Netherlands' response to the pre-draft report of the OEWG (2020), at §§ 17-18; Japan's Position Paper on the Initial "Pre-draft" of the Report of the United Nations Open-Ended Working Group on "Developments in the Field of Information and Telecommunications in the Context of International Security" (2020), at 1 and 5; Pre-Draft Report of the OEWG – ICT Comments by Austria (2020), at 2; Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security And Non-paper listing specific language proposals under agenda item "Rules, norms and principles" from written submissions received before 2 March 2020: COMMENTS FROM GERMANY (2020), at 2-3 — all available at https://www.un.org/disarmament/open-ended-working-group/. See also HRC, Res 32/13, supra note 35.

48 The Case of the S.S. Lotus, 1927 PCIJ Series A, No. 10, para 45; ILC, Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law, Report of the Study Group of the International Law Commission Finalized by Martti Koskenniemi, UN Doc A/CN.4/L.682, 13 April 2006, § 120.

49 Second "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security (2020), available at https://www.un.org/disarmament/open-ended-working-group/, § 21. See also Moynihan, 'The Application of International Law to State Cyberattacks Sovereignty and Non-intervention', Chatham House Research Paper, December 2019, paras 5-6. See also Schmitt, Tallinn Manual 2.0, supra note 6, at 31, para 4 and at 46, para 12; Nuclear Weapons, supra note 30, para 39; ILC, Draft Articles on Prevention, supra note 26, at 154, Commentary to Draft Article 3, para 11; Seabed Mining, supra note 16, para 117; Sullivan, supra note 3, at 452; Geiss and Lahmann, 'Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention', in K. Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy (2013) 621, at 655.

50 Schmitt, Tallinn Manual 2.0, supra note 6, at 31, para 4; Okwori, 'The Obligation of Due Diligence and Cyber-Attacks: Bridging the Gap Between Universal and Differential Approaches for States', Ethiopian Yearbook of International Law (2018) 205, at 213; Khanna, 'State Sovereignty and Self-Defence in Cyberspace', V(4) BRICS Law Journal (2018) 139, at 141. See, generally, Nuclear Weapons, supra note 30, para 39.

is broad, only limited by their respective triggers and subject-matter.[51] This means that, by default, positive duties established in both regimes apply to cyberspace, in the absence of specific carve-outs excluding ICTs from their scope of application. There is no evidence of such an exception, and admissible derogations from such obligations must be interpreted restrictively, due to their *erga omnes* character.[52]

On the contrary, not only have States affirmed the relevance of international law, IHRL and IHL generally in cyberspace, but they have also supported the applicability of different due diligence obligations in respect to ICTs, albeit in a fragmented way. For instance, as far back as in 2011, the then US government recognized the application of positive IHRL duties online as well as a duty to prevent cybercrime.[53] Shortly thereafter, the Council of Europe issued a Recommendation recognizing the applicability of the no-harm principle to malicious cyber activities.[54] The Explanatory Memorandum adds that this principle

> sets forth a standard of care or due diligence for the protection and promotion of integrity and universality of the Internet [...]. Under such a standard, states are required to take reasonable measures to prevent, manage and respond to significant transboundary disruptions to or interferences with the infrastructure or critical resources of the Internet.[55]

Along with the abovementioned statement by the EU representative in the context of the COVID-19 crisis — which was expressly supported

51 Nuclear Weapons, supra note 30, paras 86.
52 ILC, Fragmentation Report, supra note 48, at § 109.
53 US, International Strategy for Cyberspace, supra note 47, at 10.
54 protection and promotion of the universality, integrity and openness of the Internet (2011), available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2f8
55 Explanatory Memorandum to the draft Recommendation CM/Rec(2011)... of the Committee of Ministers to member States on the protection and promotion of Internet's universality, integrity and openness, CM Documents, CM(2011)115-add1, 24 August 2011, § 80 and more extensively §§ 71-84, available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805ccaeb. See also Interim Report of the Ad-hoc Advisory Group on Cross-border Internet to the Steering Committee on the Media and New Communication Services incorporating analysis of proposals for international and multi-stakeholder cooperation on cross-border Internet, Strasbourg, December 2010, §§ 59-74 and in particular §§ 72-74 on the standard of due diligence, available at http://humanrightseurope.blogspot.com/2011/01/proposals-for-international-cooperation.html.

by Turkey, North Macedonia, Montenegro, Serbia, Albania, Bosnia and Herzegovina, Iceland, Liechtenstein, Norway, Ukraine, Moldova and Armenia[56] — several States have recently recognised slightly different iterations of a 'cyber due diligence' rule. For instance, mirroring the Corfu Channel dictum and Rule 6 of the Tallinn Manual 2.0, France has recently stated that '[i]n accordance with the principle of due diligence, States have the obligation to not knowingly allow their territory to be used to commit acts *prohibited by international law against third States* through the use of cyber means. This obligation also applies to activities conducted in cyber space by non-state actors situated in the territory or under the jurisdiction of the State in question.'[57] Similarly, Estonia has expressed the view that 'states have to make reasonable efforts to ensure that their territory is not used to *adversely affect the rights of other States*.[58]

With a different wording, Australia has pointed out that 'to the extent that a state enjoys the right to exercise sovereignty over objects and activities within its territory, it necessarily shoulders corresponding responsibilities to ensure those objects and activities are not used to harm other states'.[59] More eloquently, Finland has stated that '[i]t is clear that States have an obligation not to knowingly allow their territory to be used for activities that cause serious harm to other States,

56 See Council of the EU, Press Release, supra note 2.

57 Emphasis added. Statement by France's Deputy Permanent Representative at the UN at the UNSC Arria-Formula Meeting on Cybersecurity, Ms. Anne Gueguen (2020), available at https://youtu.be/K704P5D1n3E, (timestamp 25:00). See also France, Droit International Appliqué, supra note 47, at 10. Cf. Developments in the field of information and telecommunications in the context of international security: Report of the Secretary-General, UN Doc. A/74/120, 24 June 2019, Reply by France, at 24; and Stratégie internationale de la France pour le numérique (2017), available at https://www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf, at 32. See also France's response to the pre-draft report from the OEWG Chair (2020), available at https://www.un.org/disarmament/open-ended-working-group/, at 3.

58 Emphasis added. Estonia, President of the Republic at the opening of CyCon 2019 (2019), available at https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html.

59 Emphasis added. Australia's Non Paper, supra note 47, at 8. See also See Australia, DFAT, Australia's International Cyber Engagement Strategy — Annex A: Australia's position on how international law applies to State conduct in cyberspace (2019), available at https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/annexes.html#Annex-A.

whether using ICTs or otherwise'.[60] It has also recognised that 'each State has to protect individuals within its territory and subject to its jurisdiction from interference with their rights by third parties'.[61] And, in what seems to combine different legal concepts, The Netherlands have posited that:

> The principle is articulated by the International Court of Justice, for example, in its judgment in the Corfu Channel Case, in which it held that states have an obligation to act if they are aware or become aware that their territory is being used for acts contrary to the rights of another state. […] It is generally accepted that the due diligence principle applies only if the state whose right or rights have been violated suffers *sufficiently serious adverse consequences.*[62]

Similar statements have been made by the Czech Republic,[63] the Republic of Korea,[64] Austria,[65] the Dominican Republic,[66] Chile, Ecuador, Guatemala, Guyana and Peru.[67] Taken together, they seem to support the view that existing due diligence obligations are fully applicable to ICTs, even if their specific implementation in cyberspace requires additional guidance.

At the same time, it remains unclear whether an all-encompassing rule or principle of due diligence exists generally in international law

60 Statement by Ambassador Janne Taalas at the second session of the open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security (2020), available at https://papersmart.unmeetings.org/media2/23732356/finland-international-law.pdf.
61 Ibid.
62 The Netherlands, Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace — Appendix: International law in cyberspace (2019), available at https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace, at 4-5.
63 Czech Republic, supra note 47, at 3.
64 Republic of Korea, Comments on the pre-draft of the OEWG Report (2020), available at https://front.un-arm.org/wp-content/uploads/2020/04/200414-rok-comment-on-pre-draft-of-oewg.pdf, at 2.
65 Austria, supra note 47, at 2-5.
66 Statement by the Dominican Republic's Ambassador and Special Envoy to the Security Council, H.E. Mr. José Singer Weisinger (2020), available at https://vm.ee/sites/default/files/Estonia_for_UN/22-5-2020_cyber_stability_and_conflict_prevention_-3.pdf.
67 OAS, Improving Transparency, supra note 46, § 58. See also §§ 56ff.

or specifically in cyberspace.[68] In particular, some have suggested that Rule 6 of the Tallinn Manual 2.0 and similar cyber-articulations of the concept are *lex ferenda*[69] or simply proposed interpretations of how an existing 'wide-ranging' due diligence obligation should apply to cyberspace.[70] There may be several reasons of policy behind States' reluctance to commit to a new rule. For instance, they may fear that too fine-grained a rule of due diligence for cyberspace would stifle it, thus removing part of its flexibility.[71] Alternatively, such a new rule may put in question the applicability and binding character of existing ones.[72] It is also possible that, by widening the scope of unlawful acts in cyberspace, a new rule of cyber due diligence could increase resort to countermeasures and litigiousness among States.[73]

Perhaps the choice of using 'due diligence' to label a range of multifaceted duties of reasonable care is misleading: its simplicity masks the complexity and diversity of international obligations requiring diligent behaviour to prevent, halt or redress certain harms, as it will be shown in the following section. Part of the confusion also seems to arise from the framing of ICTs as a new space or domain, rather than a new

68 See, e.g., The Netherlands, Letter of 5 July 2019 (Appendix), supra note 62, at 4, acknowledging that 'it should be noted that not all countries agree that the due diligence principle constitutes an obligation in its own right under international law. The Netherlands, however, does regard the principle as an obligation in its own right, the violation of which may constitute an internationally wrongful act.'

69 See Schmitt, '"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law', 19 Chicago Journal of International Law (2018) 30, at 51. See also Schmitt, Tallinn Manual 2.0, supra note 6, at 32, para 6; US, International Strategy for Cyberspace, supra note 47, at 10 (listing 'Cybersecurity Due Diligence' as an emerging norm specific to cyberspace); Intervención de la República Argentina 2° Reunión sustantiva GTCA sobre los progresos de la informática y las telecomunicaciones en el contexto de la seguridad internacional 11 de febrero de 2019 [sic] (2020), available at https://papersmart.unmeetings.org/media2/23732432/Statement-by-argentina-on-international-law.pdf.

70 See, e.g., Milanovic and Schmitt, 'Cyber Attacks and Cyber (Mis)information Operations during a Pandemic', Journal of National Security Law & Policy (forthcoming), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3612019, at 28 (arguing, that '[t]his obligation is in our view simply a cyber-articulation of a wide-ranging due diligence positive obligation under general international law requiring a State to stop harms to the rights of other States emanating from its territory', emphasis added); France, Response to the OEWG pre-draft report, supra note 57, at 1-2; Czech Republic, supra note 47, at 3.

71 Jensen and Watts, supra note 8, at 1574.

72 Austria, supra note 47, at 2; Australia's comments on the Initial "Pre-draft" of the report of the UN Open Ended Working Group in the field of information and telecommunications in the context of international security (OEWG) (2020), available at https://front.un-arm.org/wp-content/uploads/2020/04/final-australia-comments-on-oewg-pre-draft-report-16-april.pdf, at 2-3, item C2.

73 Jensen and Watts, supra note 8, at 1573-1574.

set of communication tools. However, the uncertainty surrounding a general principle or a cyber-specific version of due diligence does not mean that cyberspace is a 'duty-free zone'. For, however we label it, an existing patchwork of primary 'protective obligations' of conduct already requires States to prevent, halt and redress different types of harmful cyber operations.

4. Four Sets of Primary Duties to Prevent, Halt and/or Redress Harmful Cyber Operations

A.The Corfu Channel Principle: A Duty to Prevent Cyber Acts Contrary to the Rights of Other States

The first due diligence obligation whose applicability in cyberspace has found support among States[74] and commentators[75] alike is the 'well-recognized' Corfu Channel principle, requiring States 'not to allow knowingly its territory to be used for *acts contrary to the rights of other States*'.[76] This duty is a natural corollary of States' sovereign rights over their territory and, in essence, requires them to protect the rights of other States therein.[77] The obligation covers not only acts that directly violate the rights of third States, including their right to territory and property, but also those of their nationals, even when abroad.[78] It comprises a duty to both prevent and stop the harmful acts in question[79]

74 See supra notes 54-67.

75 See, e.g., Schmitt, Tallinn Manual 2.0, supra note 6, at 35-36, para 21; Milanovic and Schmitt, supra note 85, 28; Schmitt, 'In Defense of Due Diligence in Cyberspace', 125 The Yale Law Journal Forum (2015) 68; Bannelier-Christakis, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?', 14 Baltic Yearbook of International Law (2014) 23, at 25-26; Kulesza, 'Due Diligence in International Internet Law', Journal of Internet Law (2014) 24, at 27-28; Geiss and Lahmann, supra note 49, at 635; Gross, 'Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents', 48 Cornell International Law Journal (2015) 481, at 494; Ney and Zimmermann, 'Cyber-Security Beyond the Military Perspective: International Law, 'Cyberspace', and the Concept of Due Diligence', 58 GYIL (2015) 51, at 61-62; Walter, 'Obligations of States Before, During, and After a Cyber Security Incident', 58 GYIL (2015), 67, at 73-76; Dörr, 'Obligations of the State of Origin of a Cyber Security Incident', 58 GYIL (2015), 87, at 91-92; Jensen and Watts, supra note 8, at 1565-1566.

76 Corfu Channel, supra note 9, at 22 (emphasis added)

77 Island of Palmas, supra note 10, at 839. See also, Australia's Non Paper, supra note 47, at 8.

78 Ibid.; Affaire des biens britanniques au Maroc espagnol (Spain v UK), 1925 2 RIAA 615, at 643-644.

79 See, mutatis mutandis, Case concerning United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), Judgment, 24 May 1980, ICJ Reports (1980) 3, paras 63, 68.

and arises as soon as a State knows or should have known[80] that such act originates from or transits through its territory.[81] However, the obligation is only breached when the harm materialises.[82] In a sense, this is an obligation without a sanction for non-compliance, unless actual harm occurs. Often seen as a shortcoming, this norm structure may be explained by the need to encourage States to continuously prevent harm before their responsibility can be engaged.

Rule 6 of the Tallinn Manual 2.0 seems to contemplate a cyber-specific articulation of the Corfu Channel principle.[83] This formulation — which has been picked up by some States[84] — has four noteworthy features: i) the type of harm envisaged, ii) the threshold of harm, iii) the scope of preventive duties, and iv) the knowledge requirement.

i) Type of harm

The Commentary to Rule 6 posits that an act which 'affects the rights of other states' should be understood as an internationally wrongful act.[85] It also notes that this ought to include not only breaches of international law attributable to States, but also conduct that would have been unlawful if committed by the 'host' State, no matter its source.[86] But

80 Corfu Channel, supra note 9, at 18. On the requirement of knowledge as applied to cyberspace, see Schmitt, Tallinn Manual 2.0, supra note 6, pages 40-41.
81 Nicaragua, supra note 11, para 157.
82 See Article 14(3), ARSIWA. See also Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia-Herzegovina v. Yugoslavia), Judgment, 26 February 2007, ICJ Reports 2007 43, para 431; Bannelier-Christakis, supra note 75, at 37. Contra Antonopoulos, 'State responsibility in cyberspace', in N. Tsagourias and R. Buchan (eds), Research handbook on international law and cyberspace (2015) 55, at 69.
83 Schmitt, Tallinn Manual 2.0, supra note 6, at 30. The Manual is the result of the work of a group of experts, which purports to comprehensively analyse how international law applies in cyberspace.
84 See e.g. France's response to the pre-draft report from the OEWG Chair, supra note 57, at 3; and The Netherlands, Letter of 5 July 2019 (Appendix), supra note 62, at 4.
85 Schmitt, Tallinn Manual 2.0, supra note 6, at 34, Commentary to Rule 6, para 17. See also Submission of Australia's independent expert to the United Nations Group of Governmental Experts on advancing responsible State behaviour in cyberspace in the context of international security (GGE), Ms Johanna Weaver (2020), available at https://www.dfat.gov.au/sites/default/files/submission-by-australias-representative-to-the-gge-norm-implementation-may-2020.pdf., at 4; The Netherlands, Letter of 5 July 2019 (Appendix), supra note 62, at 4; Okwori, supra note 50, at 219-220; Sander, 'Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections', 18 Chinese Journal of International Law (2019) 1, at 25-26; Milanovic and Schmitt, supra note 72, at 27-28.
86 Schmitt, Tallinn Manual 2.0, supra note 6, at 35-36, para 21; Milanovic and Schmitt, supra note 72, at 28.

while the Corfu Channel dictum recognises State responsibility for lack of diligence in preventing or stopping acts of non-State actors regardless of attribution,[87] no reference is made to either acts merely affecting the rights of other States or fully-fledged internationally wrongful acts, i.e. breaches of international law attributable to a State. Instead, the language used in Corfu Channel is that of 'acts contrary to the rights of other states.' This language does not fully mirror the two concepts featuring in Rule 6 of the Tallinn Manual 2.0, but perhaps sits in between them.

Although most acts contrary to the rights of other States are internationally wrongful acts, the overlap is not complete. Firstly, not all acts committed by non-State groups which are contrary to the rights of other States also constitute internationally wrongful acts, or would have done so if committed by the territorial State. The Tallinn Manual 2.0 also does not clarify whether, in speculating if the conduct would have been unlawful if committed by the host State, one must consider the concrete circumstances prevailing at the time or the obligations of the host State in abstracto.[88] A second difference may concern acts that are not unlawful because of the operation of circumstances precluding wrongfulness, but would still entitle the 'victim' State to claim compensation for a material loss.[89] Thus, the framing of the type of harm covered by the Corfu Channel principle as 'internationally wrongful acts' is not entirely accurate. And neither does its qualification as 'acts that affect the rights of other states'. This is because not all conduct merely affecting the rights of third States — such as certain instances of cyber espionage[90] — necessarily contravenes their rights.

An example of an act 'contrary to the rights of other States' may be found in the United Kingdom (UK)'s recent condemnation as contrary to international law 'irresponsible activity being carried out by criminal

87 See Affaire des biens britanniques au Maroc espagnol, supra note 78, at 643-644; Koivurova, supra note 14, para 2; Dörr, supra note 75, at 90; Kolb, supra note 42, at 119.
88 Schmitt, Tallinn Manual 2.0, supra note 6, at 35-36, paras 18-22.
89 Article 27, ARSIWA.
90 See below, Section 4(A)(ii).

groups' and 'cyberattacks by States and non-States actors' during the COVID-19 pandemic.[91] The acts in question consisted of 'malicious cyber campaigns targeting international healthcare and medical research organisations involved in the coronavirus response', which were clearly contrary to the rights of States and individuals. Acts covered by the Corfu Channel principle are not limited to physical harm or damage.[92] This is particularly important in cyberspace, where many harms have no direct material impact, but undermine the operation of governmental or private functions, such as disruptions of financial or media services.[93]

ii) Threshold of harm?

Rule 6 of the Tallinn Manual 2.0 purports to be engaged only if an internationally wrongful act has 'serious adverse consequences' for other States.[94] This threshold of harm is not found in pre-existing iterations of the Corfu Channel principle. Instead, it seems to have been drawn from the no-harm principle,[95] which requires significant transboundary harm but not necessarily an act contrary to the rights of other States. Like much of the existing literature on due diligence,[96] the Manual seems to have merged the two principles into one single rule or principle of due diligence for cyberspace.[97]

91 Press release: UK condemns cyber actors seeking to benefit from global coronavirus pandemic (2020), available at https://www.gov.uk/government/news/uk-condemns-cyber-actors-seeking-to-benefit-from-global-coronavirus-pandemic.

92 Kolb, supra note 42, at 121; The Netherlands, Letter of 5 July 2019 (Appendix), supra note 62, at 5.

93 See Schmitt, Tallinn Manual 2.0, supra note 6, at 38.

94 Ibid., at 36-37, paras 25-27; at, 39, para 33. See also Okwori, supra note 50, at 218-219; Milanovic and Schmitt, supra note 72, at 28. See also The Netherlands, Letter of 5 July 2019 (Appendix), supra note 62, at 5; New Canadian text proposals (to the OEWG's initial pre-draft) (2020), available at https://front.un-arm.org/wp-content/uploads/2020/04/new-canadian-text-proposals-april-6-final.pdf, at 3.

95 Schmitt, "Virtual" Disenfranchisement, supra note 69, at 54.

96 See, e.g., Couzigou, 'Securing cyber space: the obligation of States to prevent harmful international cyber operations', 32 International Review of Law, Computers & Technology (2018), 37; Okwori, supra note 50, at 208-213; Geiss and Lahmann, supra note 49, at 635; Gross, supra note 75, at 494; Ney and Zimmermann, supra note 75, at 61-62; Walter, supra note 75, at 73-76; Dörr, supra note 75, at 91-92; Brunée and Meshel, supra note 26, at 133-135; Jensen and Watts, supra note 8, at 1565-1566.

97 Schmitt, Tallinn Manual 2.0, supra note 6, at 30-32, paras 1-5. See also Milanovic and Schmitt, supra note 72, at 28 (positing that Rule 6 of Tallinn 2.0 'is in our view simply a cyber-articulation of a wide-ranging due diligence positive obligation under general international law requiring a State to stop harms to the rights of other States emanating from its territory', emphasis added).

However, that is not to say that a failure to prevent or halt any harmful act, regardless of its gravity, amounts to a breach of the Corfu Channel principle. States are not responsible for failing to avoid minor or negligible disruptions, such as the temporary defacement of non-essential government websites. Nonetheless, this is not because the principle contains a specific threshold of harm. Rather, it is because those harms may not be contrary to the rights of other States.[98] For instance, in many circumstances, cyberespionage or the mere corruption of data — according to some — may not be contrary to the victim State's sovereign rights over its territory[99] or its right not to be subjected to foreign intervention.[100] Conversely, any lack of diligence in preventing or stopping an act of a State or private entity that contravenes the rights of other States could breach the Corfu Channel principle. And this includes acts occurring entirely within the duty-bearer's territory, as the Corfu Channel principle does not require a transboundary element.[101]

iii) Scope and aim of preventive duties

Drawing on the duty to prevent genocide, the Group of Experts involved in Tallinn 2.0 rejected the view that States have a 'general duty of prevention', that is, a duty to prevent future malicious cyber operations.[102] For the Experts, the Corfu Channel principle only applies to ongoing or at most imminent operations, at least as far as cyberspace is concerned.[103] This would limit the scope of the duty to an obligation to simply halt harmful cyber operations.[104] As a consequence, when discharging this duty, States would not be required to adopt strictly

98 Walton, supra note 34, at 1466, 1475-1477; Crootof, 'International Cybertorts: Expanding State Accountability in Cyberspace', 103 Cornell Law Review (2018) 565, at 565-567, 597-599, 606-607.
99 See Corn and Taylor, supra note 46, at 209-210. But see Schmitt, Tallinn Manual 2.0, supra note 6, at 18-19 and 171, para 10 (noting that although most acts of cyberespionage are lawful, they may constitute a breach of sovereignty if physically conducted on the territory of the victim State and attributable to another State). See also R. Buchan, Cyber Espionage and International Law (2019), at 51.
100 Schmitt, Tallinn Manual 2.0, supra note 6, at 36, para 23.
101 This position seems to have been implicitly endorsed in Schmitt, Tallinn Manual 2.0, supra note 6, at 39, para 32.
102 Ibid., at 31, para 5; at 41-42, para 42, at 44-45, paras 7, 10.
103 Ibid., at 43-44, paras 3-4. See also Okwori, supra note 50, at 216.
104 Schmitt, Tallinn Manual 2.0, supra note 6, at 44-45, para 7.

preventive, ex ante measures such as continuous supervision or monitoring of their networks.[105]

This view has been justified by the current lack of technical feasibility to prevent online harms, given their frequency and speed, as well as privacy concerns.[106] But this misses the point. Due diligence obligations, including the Corfu Channel principle, are inherently flexible. They depend on the capacity and position of each State to prevent or halt the harm in question, whether the cyber operation originates from or transits through its territory.[107] Thus, a State is not required to do the impossible, and different States may be required to adopt different measures in different circumstances.

Yet such flexibility is no excuse for inaction either. Due diligence obligations of conduct are accompanied by an obligation of result to put in place the minimum governmental infrastructure that is reasonable in the circumstances, enabling a State to exercise the necessary degree of diligence.[108] In this sense, two limbs make up the Corfu Channel principle, as well as other rules incorporating a due diligence standard.[109] First, there is an obligation of result to set up a minimal State apparatus

105 Ibid., at 44-45, paras 7 and 10; Couzigou, supra note 96, at 50-51; Okwori, supra note 50, at 215; Jensen and Watts, supra note 8, at 1566; Takano, 'Due Diligence Obligations and Transboundary Environmental Harm: Cybersecurity Applications', 36 Laws (2018) 7, at 8. See also ILA Study, supra note 18, at 7-8; Estonia, supra note 58; New Canadian text proposals, supra note 94, at 3; Ecuador preliminary comments to the Chair's "Initial pre-draft" of the Report of the United Nations Open Ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG) (2020), available at https://front.un-arm.org/wp-content/uploads/2020/04/ecuador-comments-on-initial-pre-draft-oewg.pdf, at 2.

106 Schmitt, Tallinn Manual 2.0, supra note 6, at 45, para 8. See also Okwori, supra note 50, at 215; Crootof, supra note 98, at 611, Goldsmith, Cybersecurity Treaties: A Skeptical View – Future Challenges Essay, available at https://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf (2011), at 9-10.

107 Schmitt, Tallinn Manual 2.0, supra note 6, at 47, para 16-18; Buchan, supra note 1, at 441-442; Bannelier-Christakis, supra note 75, at 37; Dörr, supra note 75, at 95. See also Ecuador preliminary comments, supra note 105, at 2; The Netherlands, Letter of 5 July 2019 (Appendix), supra note 62, at 5; Australia's Non Paper, supra note 47, at 8; New Canadian text proposals, supra note 94, at 3. On obligations of transit States, see Schmitt, Tallinn Manual 2.0, supra note 6, at 33-34, para 34.

108 See Buchan, supra note 1, at 436-437; Kolb, supra note 42, at 127, Couzigou, supra note 96, at 50-51; Takano, supra note 105, at 9.

109 Pisillo-Mazzeschi, supra note 18, at 26-27; ILC, Draft Articles on Prevention, supra note 26, at 155, Commentary to Article 3, paras 15-17.

— a core 'capacity-building' duty. Second, there is an obligation of conduct to act diligently, to the extent of a State's capacity, in preventing and halting potential or actual harmful cyberoperations. Accordingly, a State's capacity to act in cyberspace not only triggers the substantive duty to act, but also limits the required measures. Furthermore, as is the case with other due diligence obligations, the scope of States' preventive duties may change on the basis of new technological developments.[110] Thus, if a State or a corporation within its jurisdiction has or acquires the necessary technology to prevent at least some malicious cyber operations, then this State must at least try to use it as far as possible.[111] While this may raise concerns about privacy and other rights, it suffices to note that the implementation of due diligence measures under the Corfu Channel principle must be in line with international human rights law and other rules of international law.[112]

iv) Knowledge Requirement

In any event, the obligation to act in accordance with the Corfu Channel principle is only activated when a State knows or should have known about a serious risk that an unlawful cyber operation will take place, no matter how remote such risk is.[113] As the Tallinn Manual itself acknowledges, it is the actual or constructive knowledge of a serious risk that triggers due diligence obligations.[114] The decisive factor is how much information and certainty a State possesses about the harmful act in question, rather than how imminent or proximate it is. [115] The same applies to transit States, to the extent that they have actual or constructive knowledge of the risk of an unlawful cyber operation, as well as the capacity to prevent it.[116] At the same time, it does not appear that the Corfu Channel principle imposes on States a duty to actively seek knowledge of acts emanating from or transiting

110 See supra note 49.
111 See supra note 105.
112 See Bannelier-Christakis, supra note 75, at 31; Dörr, supra note 75, at 95.
113 See Kolb, supra note 42, at 123-124.
114 Schmitt, Tallinn Manual 2.0, supra note 6, at 45, para 9 and ibid., at 44-45, para 7, citing Bosnian Genocide Case, supra note 13, para 431.
115 See, mutatis mutandi, Bosnian Genocide Case, supra note 13, para 436.
116 Similarly, Couzigou, supra note 96, at 43, 47; Buchan, supra note 1, at 441. See contra Reinisch and Beham, supra note 17, at 106-107; Okwori, supra note 50, at 226-227.

through their territory which would be contrary to the rights of other States.[117] What it does require is the minimum governmental infrastructure or capacity enabling States to acquire such knowledge.[118]

In short, 'the more states can do, the more they must do',[119] and great responsibility follows inseparably from great power,[120] to the extent that such power permits. Therefore, complying with the Corfu Channel principle in cyberspace should not be an insurmountable feat: it simply requires States to build the minimum capacity that is reasonably expected of them, as well as to employ such capacity diligently in trying to protect the rights of other States and their populations, as far as possible.[121] In many circumstances, reporting and sharing information about incidents will suffice.[122]

B. The Duty to Prevent and Redress Significant Transboundary Cyber Harm

Despite their similarities, particularly a common 'capacity-to-act' requirement, the no-harm and Corfu Channel principles should be distinguished, given their distinct elements and legal consequences[123]. There are at least four significant differences between the two primary obligations: i) the type of harm; ii) the threshold of harm; iii) the legal consequences of a failure to comply with the duty, and iv) the knowledge requirement.

117 But IHRL might impose a duty to actively seek knowledge of certain threats to human rights. See Section 3(C) below.

118 See supra note 108.

119 Heieck, Symposium: A Duty to Prevent Genocide–Due Diligence Obligations among the P5 (Part One) (2018), available at http://opiniojuris.org/2018/12/10/symposium-a-duty-to-prevent-genocide-due-diligence-obligations-among-the-p5-part-one/ (emphasis added).

120 Collection Générale des Décrets Rendus par la Convention Nationale: Mois de Mai 1793 (1973), at 72. The adage has been popularized by the Spider-Man comic books, and it is widely known as the 'Peter Parker' principle (from the name of the main character's secret identity).

121 Similarly, Kolb, supra note 42, at 123

122 Gross, supra note 75, at 506

123 See ILC, State responsibility, Summary Records of the Twenty-Sixth Session, 6 May-26 July 1974, 120th Meeting, A/CN.4/Ser.A, 1974, at 7 (noting that '[i]n any case it was essential to make a very clear distinction between responsibility for wrongful activities and liability for lawful activities liable to cause damage. In the case of wrongful activities, damage was often an important element, but it was not absolutely necessary as a basis for international responsibility. On the other hand, damage was an indispensable element for establishing liability for lawful, but injurious activities', emphasis added). See also Crootof, supra note 98, at 600; Walton, supra note 34, at 1486-1487; Sander, supra note 85, at 49.

i) Type of harm

The no-harm principle does not require the infliction of an act contrary to the rights of other States but covers any 'significant transboundary harm' or the risk thereof, even if caused by lawful activities and even if no State right is undermined.[124] While some have questioned whether this obligation applies outside of the environmental legal framework, there are strong reasons to suggest that it actually covers any type of transboundary harm.[125] In particular, the Trail Smelter Arbitral Tribunal found that the obligation not to cause transboundary harm includes any 'injurious act' to the territory of another state, persons or property therein.[126] In doing so, it looked at precedents dealing not only with environmental hazards but also with the use of weapons and the treatment of aliens.[127] Similarly, according to the ICJ, the no-harm principle is a manifestation of the general principle of prevention and a natural corollary of a State's sovereignty over its territory. In the same vein, the ILC's Draft Articles on Prevention define 'harm' as 'harm caused to persons, property or the environment'.[128]

Thus, many commentators have expressed the view that the no-harm principle applies to a range of harms committed in or through cyberspace, whether or not they are contrary to the rights of other States.[129] Granted, many harmful cyber operations will be contrary to at least one rule of international law. In particular, if one views sovereignty as a standalone rule of international law, many would agree that intrusions on governmental networks or systems by another State whose agent is physically present on the victim State's territory will

124 Crootof, supra note 98, at 600; Walton, supra note 34, at 1486-1487; Sander, supra note 85, at 49. ILC, Draft Articles on Prevention, supra note 26, at 150, Commentary to Article 1, para 6; 152, Commentary to Article 2, para 5. See also Koivurova, supra note 14, para 11; Crootof, supra note 98, a 600.
125 See supra note 26 and Crootof, supra note 98, at 603-604; Walton, supra note 34, at 1465, 1479-1481; Sander, supra note 85, at 51.
126 Trail Smelter, supra note 27, at 1963.
127 Ibid., at 1963-1965.
128 ILC, Draft Articles on Prevention, supra note 26, at 152-153, Article 2(b) and Commentary, paras 8 and 9.
129 See, e.g., Crootof, supra note 98, at 603-604; Walton, supra note 34, at 1480-1482, 1497; Sander, supra note 85, a 49-50; Reinisch and Beham, supra note 17, at 104-106; Dörr, supra note 75, at 93; Buchan, supra note 1, at 439-452; Okwori, supra note 50, at 210; Takano, supra note 105. See also Interim Report of the Ad-hoc Advisory Group on Cross-border Internet, supra note 55, paras 60-65.

breach such rule.[130] Likewise, coercive interferences within a State's core governmental functions, such as its electoral processes, would violate the principle of non-intervention.[131] And to the extent that those cyber incursions violate the rights of individuals, such as their right to free elections, privacy or property, they would likely violate international human rights law.[132] This should be true at least for negative human rights obligations,[133] for which a State's jurisdiction may be triggered by the exercise of control over the activity in question,[134] the digital communications infrastructure[135] or the enjoyment of the victim's human rights,[136] regardless of physical proximity between the perpetrator and the victim.

However, no rule of international law needs to be breached or contravened for the no-harm principle to apply.[137] This gives the principle a potentially wide scope of application which is particularly well-suited for cyberspace, where debates continue as to the nature of sovereignty, jurisdiction and prohibited intervention.[138] In fact, the no-harm principle may be the only applicable rule of international law requiring States to prevent, stop and redress certain low-intensity cyber operations.[139] Although the principle requires the crossing of an

130 Schmitt, Tallinn Manual 2.0, supra note 6, at 17-20, esp. para 7; Schmitt and Vihul, 'Respect for Sovereignty in Cyberspace', 95 Texas Law Reviw (2017) 1639, at 1648-1649.
131 See, e.g., Watts, 'Low-Intensity Cyber Operations and the Principle of Non-Intervention', in J. D. Ohlin et al. (eds), Cyber War: Law and Ethics for Virtual Conflicts (2015) 250, at 257. But see Sander, supra note 85, at 20.
132 Sander, supra note 85, at 35-43.
133 See M. Milanovic, Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy (2011), at 209; Sander, supra note 85, at 39-43. On extraterritorial jurisdiction over online harms, see Section C(i) infra.
134 Sergio Euben Lopez Burgos v Uruguay, Human Rights Committee (HRC) Communication No 52/1979, UN Doc CCPR/C/13/D/52/1979, 29 July 1981, § 12.3; Lilian Celiberti de Casariego v Uruguay, HRC Communication No 56/1979, UN Doc CCPR/C/13/D/56/1979, 29 July 1981, § 10.3.
135 Report of the Office of the UN High Commissioner for Human Rights: The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37, 30 June 2014, § 34.
136 HRC, General Comment No. 36 (2018) on Article 6 of the International Covenant on Civil and Political Rights, on the Right to Life, CCPR/C/GC/36, 30 October 2018, § 63; ECtHR, Issa and Others v. Turkey, Appl. no. 31821/96, Judgment of 16 November 2004, para 71; ECtHR, Jaloud v. The Netherlands, Appl. no. 47708/08, Judgment of 20 November 2014, para 152.
137 Walton, supra note 34, at 1486. See also Finland, Statement by Ambassador Janne Taalas, supra note 61, at 2
138 Crootof, supra note 98, at 592-593; Sander, supra note 85, at 18-24, 52.
139 Walton, supra note 34, at 1497-1499, 1512.

international boundary,[140] it is not limited to physical harms.[141] Often referred to as 'international cybertorts',[142] these transboundary operations may include substantial financial loss, functional and/or physical damage to networks or systems, data corruption or loss, reputational injuries and political consequences.[143]

ii) Threshold of harm

At the same time, the no-harm principle is only engaged by significant transboundary harm or the risk thereof. In the words of the ILC:

> It is to be understood that "significant" is something more than "detectable" but need not be at the level of "serious" or "substantial". The harm must lead to a real detrimental effect on matters such as, for example, human health, industry, property, environment or agriculture in other States.[144]

'Significant harm', in this context, encompasses 'the combined effect of the probability of occurrence of an accident and the magnitude of its injurious impact'.[145] Thus, it covers activities carrying a 'low probability of causing disastrous harm', as well as operations where there is 'a high probability of causing significant harm'.[146] In cyberspace, this could potentially include online mis- and disinformation campaigns, especially those taking place during elections[147] or public health crises.[148] The

140 ILC, Draft Articles on Prevention, supra note 26, at 152-153, Article 3(c)-(e) and Commentary, paras 9-12.

141 According to the ILC, the Draft Articles were limited to physical harms 'to bring this topic within a manageable scope'. See ibid., at 151; Commentary to Article 1, para 16; Trail Smelter, supra note 27, at 1926-1927; Nuclear Weapons, supra note 30, paras 29 and 36. See also Crootof, supra note 98, at 603; Walton, supra note 34, at 1482; Buchan, supra note 1, at 449-450; Takano, supra note 105, at 1.

142 See Crootof, supra note 98, at 588-589, 592, 595-597; Walton, supra note 34, at 1513.

143 Crootof, supra note 98, at 608-609; Gross, supra note 75, at 484; Takano, supra note 105, at 6-7. See also US Government, Department of Defense Cyber Strategy (2015), available at https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf, at 5.

144 ILC, Draft Articles on Prevention, supra note 26, at 152, Commentary to Article 2, para 4 (emphasis in the original).

145 Ibid., para 2

146 Ibid., para 3.

147 See Sander, supra note 85, at 49-50.

148 See Schmitt and Milanovic, supra note 85, 2-3. See also Robinson and Spring, Coronavirus: How bad information goes viral (2020), available at https://www.bbc.co.uk/news/blogs-trending-51931394; Rankin, Russian media 'spreading Covid-19 disinformation' (2020), available at https://www.theguardian.com/

determination of what amounts to significant harm involves a subjective assessment that varies depending on the circumstances prevailing at the time, in particular, existing scientific knowledge and the economic value of the activity or good in question.[149]

iii) Knowledge requirement

Both the no-harm and the Corfu Channel principles are triggered by actual or constructive knowledge of a risk and exclude unforeseeable harms.[150] However, the no-harm principle also covers remote risks of 'disastrous harm'.[151] Thus, it may require more proactive measures of vigilance or monitoring,[152] variable on the basis of the gravity of the harm.[153] Again, a requirement to be continuously vigilant in cyberspace[154] — or any other technology or domain for that matter — depends on its technical and economic feasibility for the State in questio[155] and its compatibility with other international obligations, especially human rights. All in all, the more feasible it is for States to predict that a certain harmful cyber operation is forthcoming, the greater the degree of diligence required.

iv) Legal consequences

As seen earlier, the Corfu Channel principle is triggered once a State knows or should have known of the serious risk of an act contrary to the rights of other States emanating from or crossing its territory and is breached when the act in question occurs. It is at this point that the responsibility of the duty-bearer is engaged and other

world/2020/mar/18/russian-media-spreading-covid-19-disinformation. See also Committee on Economic, Social and Cultural Rights (CESCR), General Comment No. 14: The Right to the Highest Attainable Standard of Health (Art. 12), E/C.12/2000/4, 11 August 2000, § 34. On due diligence obligations applying in relation to COVID-19, see Coco and de Souza Dias, 'Prevent, Respond, Cooperate: States' Due Diligence Duties vis-à-vis the Covid-19 Pandemic', Journal of Humanitarian Legal Studies (2020).

149 ILC, Draft Articles on Prevention, supra note 26, at 153, Commentary to Article 2, para 7.

150 Ibid., at 153 and 155, Commentary Article 3, paras 5 and 18.

151 Ibid, at 152, Commentary to Article 2, para 3.

152 Ibid., at 156, Article 5 and Commentary.

153 Ibid., at 154-155, Commentary to Article 3, paras 11 and 18; ILA Study, supra note 18, at 12; Seabed Mining, supra note 16, para 117; Koivurova, supra note 14, para 17.

154 In defence of a duty to continuously monitor cyberspace, see Geiss and Lahmann, supra note 49, at 254-255, citing Pulp Mills, supra note 12, para. 197; Buchan, supra note 1, at 441-442; Bannelier-Christakis, supra note 75, at 30-31; Takano, supra note 105, at 7-8.

155 See Buchan, supra note 1, at 441; Gross, supra note 75, at 503.

States can respond with countermeasures. Conversely, under the no-harm principle, the occurrence of harm or the risk thereof, which a State has failed to prevent or halt, does not automatically engage the responsibility of the duty-bearer. It is only after a State fails to compensate the victim for the damage caused that a breach of the no-harm principle arises.[156]

In this way, the no-harm principle is simultaneously a primary and secondary rule of international law: it requires States to take action and also foresees the very consequences arising from a failure to act.[157] Those consequences are, first, liability for the harm caused, and, second, responsibility for the eventual failure to redress it.[158] This norm structure is a logical consequence of the principle's emphasis on reparation: States are given an opportunity to redress the harm before their responsibility is engaged. It is not the harm itself or the failure to prevent it that are unlawful,[159] but the failure to redress it. The advantages of applying this regime to cyberspace include increasing the costs of harmful cyber operations and deterring them, avoiding the stigma and antagonism associated with unlawful acts and fostering victim redress.[160]

C. The Obligation to Protect Human Rights Online

The increasing number of everyday activities which are carried out online has exposed human rights to infinite possibilities of harm. Just to mention probably the most egregious example, the right to privacy is seriously endangered by the constant tracking and mining of online activities and data, as well as their consequent profiling. Likewise, the rights to freedom of thought, information and expression may be undermined by online disinformation campaigns, the proliferation of

156 See Crootof, supra note 98, at 603; Walton, supra note 34, at 1487-1488; Sander, supra note 85, at 51; Dörr, supra note 75, at 96.
157 Walton, supra note 34, at 1486-1487; Sander, supra note 85, at 50.
158 ILC, Draft Articles on Prevention, supra note 26, at 148, General Commentary, para 1; at 150, Commentary to Article 1, para 6. See also Walton, supra note 34, at 1486-1488; Sander, supra note 85, at 51.
159 See ILC, Draft Articles on Prevention, supra note 26, at 154, Commentary to Article 3, para 7.
160 Crootof, supra note 98, at 597-599, 604-608, 614; Walton, supra note 34, at 1511-1516.

fake news or censorship. Cyber-bulling, defamation and hate speech can spread incredibly quickly, with detrimental effects on individuals' rights and reputation.[161]

International human rights law (IHRL) imposes on States a set of protective obligations against these harms. They cover online activities to the extent that they take place under a State's jurisdiction.[162] In the cyber realm as in any other area of human activity, States have not only a 'negative' duty to respect human rights online — i.e. not to violate them with their own actions such as wrongful censorship or wrongful surveillance. They also have a positive duty to adopt all reasonable measures to protect the human rights of persons under their jurisdiction against threats posed by other entities, be them foreign governments, companies, criminals, or any other actor.[163] In addition, States must ensure the effective enjoyment of human rights on the Internet.[164] Positive obligations to protect and ensure may be potentially identified for all human rights.[165] With specific reference to the rights which are more commonly endangered online, one may highlight the rights to privacy,[166] honour and reputation,[167] and freedom of information and

161 ECtHR, Delfi v Estonia, Appl. no. 64569/09, Judgment of 16 June 2015, para 110.
162 UN GGE Report 2015, supra note 5, § 28(b).
163 ECtHR, Bărbulescu v. Romania, Appl. no. 61496/08, Judgment of 12 January 2016, para 110, with respect to the right to privacy. In this sense, see also Milanovic and Schmitt, supra note 72, at 20ff.
164 Cf. HRC, General comment no. 31 [80], The nature of the general legal obligation imposed on States Parties to the Covenant, UN Doc CCPR/C/21/Rev.1/Add.13, 26 May 2004, § 8. See also HRC, CESCR General Comment No. 3: The Nature of States Parties' Obligations (Art. 2, Para. 1, of the Covenant), E/1991/23, 14 December 1990, § 1; IACtHR, Velasquez Rodriguez v. Honduras, Judgment (Merits), 29 July 1988, paras 166–167.
165 See, e.g., Article 2(1)-(2) International Covenant on Civil and Political Rights 1966, 999 UNTS 171 (ICCPR); Article 2(1), International Covenant on Economic, Social and Cultural Rights 1966, 993 UNTS 3 (ICESCR); Article 1(1), American Convention on Human Rights 1978, OAS Treaty Series No 36, 1144 UNTS 123 (ACHR); Article 1, European Convention for the Protection of Human Rights and Fundamental Freedoms1953, ETS 5 (ECHR).
166 ECtHR, X and Y v. the Netherlands, Appl. no. 8978/80, Judgement of 26 March 1985, para 23; Bărbulescu, supra note 163, para 108; ECtHR, Hämäläinen v. Finland, Appl. no. 37359/09, Judgment of 16 July 2014, para 62; ECtHR, Nicolae Virgiliu Tănase v. Romania, Appl. no. 41720/13, Judgment of 25 June 2019, para 125. Cf. also HRC, CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, UN Doc HRI/GEN/1/Rev.9, 8 April 1988, § 10.
167 HRC, General Comment 16, supra note 166, §§ 1 and 11. The principles established therein, even though not referred to information and communication technologies specifically, are in principle applicable to such technologies as well.

expression.[168] Due diligence, in this context, designates the standard of conduct which States are required to exercise to comply with the said positive obligations.[169]

Unlike the Corfu Channel and no-harm principles, IHRL due diligence duties are owed not only to States, but also individuals and the international community as a whole. However, similarities also exist among those due diligence duties: positive obligations to protect human rights require State to prevent threats to their enjoyment, halt harms once they begin and mitigate their effects, to the extent possible.[170] Likewise, as for the other examined due diligence duties, States' obligations to prevent human rights violations alleviate some of the difficulties with identifying and attributing authorship of malicious cyber operations: all that must be demonstrated is that the duty-bearer State failed to adopt the necessary and reasonable protective measures, irrespective of who or what caused the harm.[171]

States' obligations of due diligence under IHRL must not be confused with the related concept of 'human rights due diligence' — one of the non-binding responsibilities that businesses are advised to observe in mitigating the human rights impact of their activities.[172] That being said, States themselves may have a due diligence obligation to establish a legal framework that requires businesses to, in turn, exercise their own due diligence.[173]

168 HRC, General comment No. 34, Article 19: Freedoms of opinion and expression, UN Doc CCPR/C/GC/34, 12 September 2011, §§ 12, 15.
169 HRC, General Comment 31, supra note 164, § 8; Besson, supra note 44, at 2, 4-5; Schmitt and Milanovic, supra note 85, at 20, 27, 29.
170 With respect to civil and political rights, see HRC, General Comment 31, supra note 164, §§ 8, 17; for economic, social and cultural rights, see, e.g. CESCR, General comment No. 24 (2017) on State obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities, UN Doc E/C.12/GC/24, 10 August 2017, § 14.
171 Seibert-Fohr, 'From Complicity to Due Diligence: When Do States Incur Responsibility for Their Involvement in Serious International Wrongdoing?', 60 GYIL (2017) 667, at 670; Keller and Walther, 'Evasion of the international law of State responsibility? The ECtHR's jurisprudence on positive and preventive obligations under Article 3', The International Journal of Human Rights (2019) 1, at 3; HRC, General Comment 31, supra note 164, § 8.
172 On this principle, see Bonnitcha and McCorquodale, 'The Concept of 'Due Diligence' in the UN Guiding Principles on Business and Human Rights', 28(3) European Journal of International Law (EJIL) (2017) 899; and Ruggie and Sherman, 'The Concept of 'Due Diligence' in the UN Guiding Principles on Business and Human Rights: A Reply to Jonathan Bonnitcha and Robert McCorquodale', 28(3) EJIL (2017) 921.
173 CESCR, General Comment 24, supra note 170, §§ 16-18, with respect to economic, social and cultural

While States' due diligence duties under IHRL are also subject to a requirement of capacity to act, common to other due diligence obligations,[174] they may be 'substantively … more demanding' than those deriving from general international law, often including duties to actively seek knowledge of violations.[175] Positive obligations to protect human rights have other distinctive features, namely i) their limitation to the extent of the duty-bearer's jurisdiction; ii) the type of harms covered; iii) the knowledge required to trigger the obligation; as well as iv) the particular legal consequences of a failure to protect applicable human rights.

i) State Jurisdiction

Under some IHRL treaties, before States' positive obligations in respect of online or offline harms can be triggered, jurisdiction over the right in question must be established.[176] In IHRL, the concept of jurisdiction includes not only the territory of the duty-bearer but also certain physical spaces, persons or events located extraterritorially. Considering the multi-layered and transnational nature of cyberspace, comprising physical infrastructure, logical systems and human activity across multiple boundaries,[177] extraterritorial models of jurisdiction are particularly relevant in the context of States' duties to prevent online harms.

First, there is broad agreement that extraterritorial jurisdiction 'follows' individuals wherever a State exercises some form of control or authority over them.[178] This is what is known as the 'personal' model of extraterritorial jurisdiction and most human rights bodies and commentators agree that it applies to both negative and positive human

rights — but with a principle that could be extended to civil and political rights as well; Besson, supra note 44, at 8.

174 Besson, supra note 44, at 5-7.

175 Milanovic and Schmitt, supra note 85, at 30, citing as an example CESCR, General Comment 24, supra note 170, § 33.

176 See, e.g., Article 2(1), ICCPR; Article 1, ECHR; Article 1(1), ACHR.

177 Sullivan, supra note 3, at 454, fn 88.

178 HRC, General Comment 31, supra note 164, § 10.

rights obligations.[179] As is well-known, control over individuals may be exercised through the activities of State agents abroad.[180]

Second, although not without contestation,[181] several human rights bodies have expressed the view that jurisdiction may also be extended extraterritorially by looking at the activities of entities, such as companies, which are incorporated or located in the duty-bearer's territory or are otherwise subject to its control. Under this approach, a State has jurisdiction over the activities of the said entities when these have a direct and reasonably foreseeable impact on the human rights of individuals extraterritorially.[182] As such, a State's positive duties concern the rights that may be infringed by said private entities.[183]
Third, the Human Rights Committee has advanced a more expansive approach to extraterritorial jurisdiction, grounded in the exercise of control over the enjoyment of the rights in question, regardless of any physical control over territory, the perpetrators or the individual victim.[184] While this functional approach to jurisdiction[185] has been

179 M. Milanovic, Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy (2011), at 119. But the ECtHR has been reluctant to recognize this model in relation to extraterritorial kinetic force in the absence of governmental control (see ECtHR, Banković and others v. Belgium and others, Appl. no 52207/99, Decision of 12 December 2001, paras 74-82; and ECtHR, Al-Skeini and others v. United Kingdom, Appl. no 55721/07, Judgment of 7 July 2011, paras 136-137). For a recent analysis, see Milanovic, 'The Murder of Jamal Khashoggi: Immunities, Inviolability and the Human Right to Life', 20 Human Rights Law Review (2020) 1, at 23-24.
180 See e.g. Inter-American Commission on Human Rights (IAComHR), Coard et al. v. United States, Report N. 109/99, 29 September 1999, para 37; Al-Skeini, supra note 179, paras 136-139.
181 See Besson, supra note 44.
182 HRC, General Comment 36, supra note 136, § 22, with respect to the right to life; CESCR, General Comment 14, supra note 148, § 39; CESCR, General Comment No. 15: The Right to Water (Arts. 11 and 12 of the Covenant), UN Doc E/C.12/2002/11, 20 January 2003, § 33; CESCR, Statement on the Obligations of States parties regarding the corporate sector and economic social and cultural rights, UN Doc E/C.12/2011/1, 20 May 2011, § 5; IACtHR, Advisory Opinion OC-23/17 of November 15, 2017 Requested by the Republic of Colombia: The Environment and Human Rights, 15 November 2017, paras 101-102. See also Milanovic and Schmitt, supra note 85, at 29-30.
183 Although this model of jurisdiction may overlap with the requirement of a State's capacity to act, the two are grounded in different criteria and underlying rationales. Jurisdiction captures the connection between the State and the protected human right on the basis of effective control over different aspects of this connection. Conversely, capacity to act limits a State's due diligence duties on the basis of a range of factors, including control over the activities or perpetrators in question, or a less demanding ability to influence their behaviour. Contra Besson, supra note 44, at 2.
184 HRC, General Comment 36, supra note 136, § 63.
185 See Shany, 'Taking Universality Seriously: A Functional Approach to Extraterritoriality in International Human Rights Law', 7 The Law & Ethics of Human Rights (2013) 47.

accepted in respect of negative human rights duties,[186] many oppose its applicability to positive human rights obligations, fearing the lack of necessary governmental infrastructure or powers beyond a State's territory or spatial control.[187] However, the practical impact of adopting such jurisdictional model for positive obligations should not be overstated: any due diligence obligation only extends insofar as the duty-bearer has the capacity to adopt the protective or preventive measures in question.[188] Capacity, in this context, includes the ability to influence the behaviour of the perpetrators,[189] the unpredictability of certain events, the availability of resources, and the duty to respect and protect other human rights.[190] Of course, there is a difference between a State having no jurisdiction at all and it being incapable to protect human rights within its jurisdiction: in the latter situation, a preliminary assessment of the State's capacity to act, along with other triggering elements of the obligation, is required to evaluate compliance with IHRL. Still, States are not required to do the impossible or to discharge a 'disproportionate burden'[191] but are expected to adopt measures that are available and reasonable in the circumstances.[192] Thus, as in any other jurisdictional model, the requirement of capacity to act overlaps with and modulates the notion of extraterritorial jurisdiction over the enjoyment of human rights.[193]

186 Milanovic, Extraterritorial Application, supra note 179, at 209; Goodman, Heyns and Shany, Human Rights, Deprivation of Life and National Security: Q&A with Christof Heyns and Yuval Shany on General Comment 36 (2019), available at https://www.justsecurity.org/62467/human-life-national-security-qa-christof-heyns-yuval-shany-general-comment-36/ https://www.justsecurity.org/62467/human-life-national-security-qa-christof-heyns-yuval-shany-general-comment-36/, at 1-2; HRC, Sergio Euben Lopez Burgos v Uruguay, supra note 134, § 12.3; Lilian Celiberti de Casariego v Uruguay, supra note 134, § 10.3; Issa and others v. Turkey, supra note 136, § 71.

187 See, e.g., the account of the debate in Milanovic, The Murder of Jamal Khashoggi, supra note 179, at 19-20; and Milanovic, Extraterritorial Application, supra note 179, at 209, 210-212, 219-220.

188 For example, the ICESCR has no express jurisdictional threshold and yet most of its obligations are positive ones, i.e. duties to protect and ensure social, economic and cultural human rights.

189 Bosnian Genocide, supra note 13, para 430.

190 Cf. ECtHR, Osman v. United Kingdom, 87/1997/871/1083, Judgment of 28 October 1998, para 116.

191 Ibid.; see also Tănase v. Romania, supra note 166, para 136.

192 ECtHR, McCann and Others v. United Kingdom, Appl. no. 19009/04, Judgment of 27 September 1995, para 151; Velasquez Rodriguez v. Honduras, supra note 164, para 167. See also The Netherlands, Letter of 5 July 2019 (Appendix), supra note 62, at 4; and Korea, supra note 64, at 5.

193 Besson, supra note 44, at 5.

ii) Type of harm

Due diligence obligations under IHRL cover a wide spectrum of harms, including any conduct by public or private entities that impairs the enjoyment of the relevant human rights online or offline, such as the rights to privacy and freedom of expression. Unlike the no-harm principle, the online harm in question need not have a transboundary nature: provided jurisdiction is established, a State must protect relevant human rights regardless of the harm's origin or trajectory.

iii) Knowledge requirement

The amount of possible threats to the enjoyment of human rights is infinite. Thus, it would be unrealistic and unreasonable to expect a State to be in a position to adopt preventive measures against any threat or harm to human rights. Rather, States are only capable and thus required to act in the presence of some level of knowledge that there is a risk to human rights. With respect to the right to life, the Human Rights Committee and the Inter-American Court of Human Rights have stressed that the knowledge requirement consists of reasonable foreseeability of threats of harm' [194] and constructive knowledge of an immediate and certain risk,[195] respectively. Whilst these pronouncements were concerned with the protection of the right to life, there appears to be no particular reason not to extend them to positive obligations to protect other human rights, including in cyberspace. This means that, under IHRL, States must also exercise 'due diligence' in seeking and evaluating available information about threats to human rights under their jurisdiction.[196]

iv) Legal consequences of a failure to protect human rights

Unlike the Corfu Channel and the no-harm principles, positive obligations to protect and ensure human rights are breached by the mere lack of diligence, i.e. the wrongful omission or inaction in adopting

194 , § 21; cf. also Osman v. United Kingdom, supra note 190, paras 115-116.
195 IACtHR, Sawhoyamaxa Indigenous Community v. Paraguay, Judgment (Merits, Reparations and Costs), 29 March 2006, § 155; cf. very similar language in Tănase v. Romania, supra note 166, para 136.
196 HRC, General Comment 36, supra note 136, §§ 13, 23, 27.

the measures required.[197] This is true to the extent that States must prevent objectively foreseeable threats to human rights.[198] Thus, a breach of such duty arises from the emergence of a risk of harm, regardless of whether or not it materialises.[199] Although the actual occurrence of the prohibited harm is generally indicative that the State has failed to fulfil its positive obligations, proof of causation between the lack of due diligence and the harm is unnecessary. Nonetheless, in the past, the ECtHR has considered that State's knowledge of, acquiescence or connivance to human rights violations perpetrated by third parties suffices to demonstrate a breach of that State's positive duties to protect those rights.[200]

Importantly, a breach of positive human rights obligations arises not only from complete inaction but also from the adoption of insufficient or ineffective measures, when more appropriate ones would have been available[201] Conversely, the occurrence of the prohibited harm does not necessarily mean that the State violated its due diligence obligations under IHRL. A violation only arises if it is proven that the State failed to adopt additional protective measures that it could have reasonably implemented.[202]

197 See, e.g., ibid., § 7.

198 Todeschini, The Human Rights Committee's General Comment No. 36 and the Right to Life in Armed Conflict (2019), available at http://opiniojuris.org/2019/01/21/the-human-rights-committees-general-comment-no-36-and-the-right-to-life-in-armed-conflict/.

199 This principle applies at the very least to the right to life and the right not to be subjected to torture and ill-treatment (see, e.g., HRC, General Comment 36, supra note 136, § 7; ECtHR, Keller v. Russia, Appl. no. 26824/04, Judgment of 17 October 2013, para 82; Osman v. United Kingdom, supra note 190, para 116; ECtHR, O'Keeffe v. Ireland, Appl. no. 35810/09, Judgment of 28 January 2014, paras 16, 162; ECtHR, Kurt v. Turkey, Appl. no. 15/1997/799/1002, Judgment of 25 May 1998, para 69. It also seems to apply to the right to non-discrimination, including in the context of online hate speech (see Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc A/74/486, 9 October 2019, §§ 13, 14(f), 16). See, generally, Stoyanova, 'Fault, Knowledge and Risk Within the Framework of Positive Obligations Under the European Convention on Human Rights', Leiden Journal of International Law (2020).

200 See European Commission of Human rights (EComHR), Yaşa v. Turkey, Appl. no. 22495/93, Report, 8 April 1997, paras 106-107; ECtHR, Özgür Gündem v. Turkey, Appl. no. 23144/93, 16 March 2000, paras 38-46; ECtHR, Kılıç v. Turkey, Appl. no. 22492/93, Judgment of 28 March 2000, paras 57, 64, 68; ECtHR, Mahmut Kaya v. Turkey, Appl. no. 22535/93, Judgment, 28 March 2000, paras 74, 80, 85-92; all of which are discussed in Milanovic, State Acquiescence or Connivance in the Wrongful Conduct of Third Parties in the Jurisprudence of the European Court of Human Rights (2020), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3454007, at 3-6.

201 Cf. ECtHR, Hatton v UK, Appl. no. 36022/97, Judgment of 8 July 2003, paras 138-142.

202 Cf. ECtHR, E. and others v UK, Appl. no. 33218/96, Judgment of 26 November 2002, paras 99-100.

D. Cyber Due Diligence in International Humanitarian Law

Cyber operations are by now part and parcel of modern warfare. Whilst they may specifically target military infrastructure, cyber weapons and tactics have the potential to intentionally or indiscriminately[203] disable civilian infrastructure and disrupt the provision of services essential to the civilian population. Many States[204] and most commentators agree that, at the very least, cyber operations having kinetic effects similar to those of traditional uses of armed force — e.g. the destruction of civilian objects or harm to civilians — are covered by the provisions of international humanitarian law (IHL) when carried out during an armed conflict.[205] But it remains unclear whether, in the absence of physical damage, the mere corruption of data or functional system disruptions amount to attacks governed by IHL.[206] In any event, numerous rules of IHL establish obligations of conduct with which States must comply by exercising due diligence,[207] some of which require them to prevent violations or harmful activities carried out by third parties. Of particular relevance are the obligations to: i) ensure respect for IHL; and ii) adopt defensive precautions to avoid or minimize harm to civilian objects and the civilian population.

203 International Committee of the Red Cross (ICRC), Position Paper — International Humanitarian Law and Cyber Operations during Armed Conflicts (2019), available at https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts, at 5.
204 E.g., United Kingdom (UK) Attorney General's Office, Cyber and International Law in the 21st Century (2018), available at https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century; United States Comments on the Chair's Pre-draft of the Report of the UN Open Ended Working Group (2020), available at https://front.un-arm.org/wp-content/uploads/2020/04/oewg-pre-draft-usg-comments-4-6-2020.pdf, at 2; Joint Statement from Denmark, Finland, Iceland, Sweden and Norway, supra note 2.
205 E.g., Schmitt, Tallinn Manual 2.0, supra note 6, rule 82, para 16; Nuclear Weapons, supra note 30, para 86. See also Durham, Cyber operations during armed conflict: 7 essential law and policy questions (2020), available at https://blogs.icrc.org/law-and-policy/2020/03/26/cyber-armed-conflict-7-law-policy-questions/.
206 See Rödenhauser, Hacking Humanitarians? IHL and the protection of humanitarian organizations against cyber operations (2020), at https://www.ejiltalk.org/hacking-humanitarians-ihl-and-the-protection-of-humanitarian-organizations-against-cyber-operations/.
207 See Longobardo, 'The Relevance of the Concept of Due Diligence for International Humanitarian Law', 37 Wisconsin International Law Journal (2020) 44; and Berkes, 'The Standard of 'Due Diligence' as a Result of Interchange between the Law of Armed Conflict and General International Law', 23(3) Journal of Conflict & Security Law (2018) 433.

i) The General Duty to Ensure Respect for International Humanitarian Law in Cyberspace

A due diligence obligation is codified in Article 1 common to the 1949 Geneva Conventions on the protection of victims of war (GCs), which requires States to respect and ensure respect for the provisions of the conventions[208] — a provision repeated almost verbatim in Article 1(1) of Additional Protocol I (AP).[209] The customary status of this rule was recognized by the ICJ, as well as its application to both international and non-international armed conflict[210] Given the erga omnes nature of IHL, not only parties to an armed conflict, but all States are bound to do 'everything in their power to ensure that the humanitarian principles underlying the Conventions are applied universally'.[211] According to Rule 144 of the International Committee of the Red Cross (ICRC)'s Customary IHL Study,[212] this obligation requires States not only to refrain from committing or encouraging violations of IHL[213] but also to take positive steps to ensure — even in peacetime[214] — that other entities comply with IHL thereby preventing such violations from occurring.[215]

208 Article 1 common to: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field 1949, 75 UNTS 31; Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea 1949, 75 UNTS 85; Convention (III) relative to the Treatment of Prisoners of War 1949, 75 UNTS 135; Convention (IV) relative to the Protection of Civilian Persons in Time of War, 75 UNTS 287.

209 Article 1(1), Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts 1977 (AP I), 1125 UNTS 3.

210 Nicaragua, supra note 11, para 220; ICRC, Commentary on the First Geneva Convention (2016), available at https://ihl-databases.icrc.org/ihl/full/GCi-commentary, Article 1 - Respect for the Convention, at paras 125-126.

211 ICRC, Geneva Convention Relative to the Protection of Civilian Persons in Time of War: Commentary (1958), at 16; Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 9 July 2004, ICJ Reports (2004) 136, at paras 158-159.

212 J.-M. Henckaerts and L. Doswald-Beck (eds), Customary International Law — Volume I: Rules (2009), at 509-513. Rule 139, instead, reproduces verbatim the language of common Article 1, but it limits its scope of application to armed forces and other entities acting on the instructions, or under the direction or control of a party to the conflict. See ibid., at 495ff.

213 ICRC, 2016 Commentary, supra note 210, paras 154 and 158-163.

214 Ibid., paras 127-128 and 185.

215Ibid., paras 121, 153-154 and 164-173. On this obligation generally, see Dörmann and Serralvo, 'Common Article 1 to the Geneva Conventions and the obligation to prevent international humanitarian law violations', 96 International Review of the Red Cross (IRRC) (2014) 707. See also Longobardo, supra note 207, at 57-60; and Berkes, supra note 207, at 442. Contra, see Zych, 'The Scope of the Obligation to Respect and to Ensure Respect for International Humanitarian Law', 27(2) Windsor Yearbook of Access to Justice

This obligation also applies in cyberspace and entails a duty to act, as far as possible, to prevent and halt cyber operations constituting violations of IHL. Its broad scope of application covers potential violations by State agents, as well as private entities over which a State exercises authority, such as populations under belligerent occupation[216] or exerts a reasonable degree of influence, including other States and non-State groups located in different parts of the world.[217] As with other due diligence obligations, the duty to respect and ensure respect for IHL is triggered and limited by a State's capacity to act.[218] This, in turn, depends on a range of factors, such as available resources, the gravity of the violation and the degree of control or influence that the State exercises over the direct perpetrators.[219] Yet, lack of military, economic or other resources does not exempt States from what remains a binding legal obligation to acquire and employ all reasonable means to ensure respect for IHL, even in cyberspace.[220] The duty is triggered not only by a State's knowledge of violations but also by objective foreseeability.[221] Nonetheless, although the duty to prevent violations of IHL arises from the moment they become known or foreseeable, it may be argued that — as with the Corfu Channel and no-harm principles — it is only breached if the actual harm materializes.[222] States may comply with this rule by simply adopting measures well-known in the law of State responsibility, such as invoking a breach of IHL by a third State through adjudicative or diplomatic means,[223] demanding its cessation, guarantees

(2009) 251; and V. Robson, 'The Common Approach to Article 1: The Scope of Each State's Obligation to Ensure Respect for the Geneva Conventions', 25(1) Journal of Conflict and Security Law (2020) 101. On examples of operational measures, see European Union, Updated European Union Guidelines on promoting compliance with international humanitarian law, 15 December 2009, 2009/C 303/06, § 16.

216 ICRC, 2016 Commentary, supra note 210, para 150.

217 Ibid., paras 150 and 153-154.

218 Ibid., paras 166, 187.

219 Ibid., paras 165-166 and, mutatis mutandis, Bosnian Genocide, supra note 13, para 430. See also Longobardo, supra note 207, at 60-62.

220 ICRC, 2016 Commentary, supra note 210, para 187.

221 Ibid., paras 150, 164.

222 ICRC, 2016 Commentary, supra note 210, para 166 establishes a parallelism between common Article 1 and Article 1 of the 1948 Genocide Convention. The ICJ in Bosnian Genocide, supra note 13, para 431, established that a breach of the duty to prevent occurs only if genocide is actually committed, in line with Article 14(3) ARSIWA.

223 ICRC, 2016 Commentary, supra note 210, para 181.

of non-repetition or reparations,[224] refraining from recognizing the situation as lawful and rendering aid and assistance to the State in breach,[225] as well as taking effective steps to investigate and repress the violations.[226]

ii) The Duty to Adopt Protective Precautions against the Effects of Cyber Warfare

The principle of precaution enshrined in several IHL provisions also embodies a set of due diligence duties to protect individuals against harm. Article 51 AP I generally provides that "[t]he civilian population and individual civilians shall enjoy general protection against dangers arising from military operations."[227] It is immediately evident how cyber warfare may pose a challenge to the application of such rule. To begin with, civilian cyberinfrastructures may not be easily distinguishable from lawful military objectives, as these often depend on services and resources provided by private entities.[228] The interconnectivity of cyberspace may also mean that cyberattacks directed against military objectives may spill over civilian systems, causing disruption or dysfunctionality.[229]

To obviate such undesirable results, Article 58 AP I requires parties to a conflict to adopt precautionary measures to protect civilian populations and objects against the effects of attacks, provided they exercise control over the territory, physical infrastructure or perhaps the operational system which may be targeted.[230] The rule has achieved

224 Article 48, ARSIWA. Cf. ICRC, Memorandum from the International Committee of the Red Cross to the States Parties to the Geneva Conventions of August 12, 1949 concerning the conflict between Islamic Republic of Iran and Republic of Iraq (1983), available at https://casebook.icrc.org/case-study/icrc-iran-iraq-memoranda.

225 Articles 16 and 40-41, ARSIWA; cf. ICRC, 2016 Commentary, supra note 210, paras 158-163.

226 Koivurova, supra note 14, para 32.

227 Article 51, AP I. See generally Jensen, 'Precautions against the effects of attacks in urban areas', 98 IRRC (2016) 147; Quéguiner, 'Precautions under the law governing the conduct of hostilities', 88 IRRC (2006) 793.

228 Cf. Article 52(2), AP I.

229 See Gisel and Rodenhäuser, Cyber operations and international humanitarian law: five key points (2019) available at https://blogs.icrc.org/law-and-policy/2019/11/28/cyber-operations-ihl-five-key-points/

230 Y. Sandoz, C. Swinarski and B. Zimmermann, Commentary on the Additional Protocols of 8 June 1977

customary status, as recognised by Rules 22-24 of the ICRC's Study on Customary IHL, and is applicable not only in international armed conflicts but also, arguably, in non-international ones.[231]

Along with other due diligence obligations, the duty to adopt precautions against the effects of attacks is triggered and limited by a State's capacity to act, only covering measures that are 'practicable or practically possible'.[232] In respect of cyberattacks, this might require States to adopt, to the extent feasible, measures such as establishing a clear separation between military and civilian cyberinfrastructure and networks, identifying and protecting critical civilian infrastructure and services — such as those related to the provision of medical assistance, electricity, telecommunications, transport and distribution of objects indispensable for the survival of civilians — from potentially disruptive cyber operations, such as by taking them off the Internet.[233]

to the Geneva Conventions of 12 August 1949 (1987), at 692, para 2239.
231 Henckaerts and Doswald-Beck, supra note 212, at 69-70.
232 Cf., e.g., US Department of Defense, Law of War Manual, June 2015 (Updated December 2016), at 192, § 5.2.3.2.
233 Cf. ICRC, Position Paper, supra note 203, at 6. See also Mačák, Gisel and Rodenhäuser, Cyber Attacks against Hospitals and the COVID-19 Pandemic: How Strong are International Law Protections? (2020), available at https://www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/.

5. By Way of Conclusion: A Patchwork of Primary Cyber Due Diligence Duties

Throughout this contribution, we have stressed that the concept of due diligence is best understood as a flexible standard of care or good governance found in a variety of primary rules or principles of international law across a range of areas. Thus, in a way, there is a patchwork of different but overlapping due diligence obligations governing cyberspace. Yet a set of core elements also threads them together.

First, all due diligence obligations seem to presuppose the exercise of State sovereignty, jurisdiction or control over a territory, the right-holder or the conduct in question.[234] Secondly, and relatedly, those obligations are subject to and limited by a State's capacity to act,[235] giving effect to the idea that States have common but differentiated responsibilities.[236] Thirdly, this flexible obligation of conduct is coupled with an obligation of result[237] to put in place the minimal legislative, judicial and executive infrastructure needed to exercise due diligence.[238] Fourthly, a State is only required to act in the presence of some degree of information about the harm or risk in question, ranging from actual or constructive knowledge to objective foreseeability.[239] Lastly, all these elements are geared towards a central duty to prevent, halt and/or redress harm or the risk thereof, consisting of an act contrary to the rights of other States, significant transboundary harm, or a violation of more specific international rules, such as IHRL and IHL.

234 ILA Study, supra note 18, at 5; HRC, General Comment 36, supra note 136, § 22.
235 Alabama, supra note 20, at 129; ILA Study, supra note 18, at 20, 47; HRC, General Comment 36, supra note 136, § 21; Bosnian Genocide, supra note 13, paras 430-432; Nicaragua, supra note 11, para 157. See also Koivurova, supra note 14, paras 17, 19
236 Koivurova, supra note 14, para 19.
237 Pisillo-Mazzeschi, supra note 18, at 27.
238 ILC, Draft Articles on Prevention, supra note 26, at 155-156; Commentary to Article 3, para. 17; Article 5 and Commentary; ILA Study, supra note 18, at 124; Alabama Claims Commission, 131; Koivurova, supra note 14, para 21; Pisillo-Mazzeschi, supra note 18, at 26–27; Kolb, supra note 42, at 117, 127; Couzigou, 50-51; Okwori, 223. Krieger & Peters.
239 ILA Study, supra note 18, at 47.

These common threads raise the following question, foreshadowed at the beginning of this paper: is there a general principle of due diligence in international law? Perhaps. This is what the ICJ seemed to be implying when, in Pulp Mills, it stated that 'the principle of prevention is a customary rule, and as such it has its origins in the [standard of] due diligence that is required of a State in its territory'.[240] In the same vein, citing the Alabama Claims Commission, the Trail Smelter Arbitral Tribunal held that both arbitrations were decided on the basis of the 'same general principle' according to which '[a] State owes at all times a duty to protect other States against injurious acts by individuals from within its jurisdiction'.[241] The ILA[242] and some States have also supported this position, particularly in the context of cyberspace. But whether or not this holds true, it should not detract from the fact that a comprehensive legal framework of binding due diligence obligations already applies in cyberspace,[243]no matter how patchy or fragmented it is.

Such framework comprises at least two different primary rules of general application, namely the Corfu Channel and the no-harm principles. In addition, different obligations of due diligence arising under specialized branches of international law apply concurrently to cover different uses, aspects and consequences of ICTs. Among them we have highlighted the positive obligation to protect human rights online, as well as the duty to ensure respect for IHL and to adopt precautions against the effects of cyberattacks in armed conflict.

While the said rules overlap and could be interpreted systematically insofar as they work towards similar goals, they remain separate and should not be conflated. Each has different triggers, requirements and standards of care. It may well be that, from their similarities,

240 Emphasis added. Pulp Mills, supra note 12, para 101. See also ILA Study, supra note 18, at 6; Koivurova, supra note 14, para 41; Couzigou, supra note 96, at 39; Hankinson, Due Diligence and the Gray Zones of International Cyberspace Laws (2018), available at http://www.mjilonline.org/due-diligence-and-the-gray-zones-of-international-cyberspace-laws/.

241 Trail Smelter, supra note 27, at 1963 and 1965.

242 ILA Study, supra note 18, at 6.

243 See, e.g., France, Response to the OEWG pre-draft report, supra note 57, at 3; Korea, supra note 64, at 2, 5.

one can derive a general principle of international law. Furthermore, States maintain the prerogative to develop — through conventional or customary international law — a new specialised duty of 'cyber due diligence'. This duty may well be modelled on any of the existing due diligence obligations or a mix thereof, following the approach of the Tallinn Manuals. But, in debates about 'cyber due diligence', the controversial existence of a general principle or a cyber-specific rule of due diligence should not be presented as an alternative to a legal vacuum. For international law already provides more than meets the eye: a patchwork of due diligence duties that, together, require States to do their best to prevent, halt and respond to a wide range of online harms.

Core Due Diligence Principle and its Link to the Duty to Cooperate

*Tomohiro Mikanagi**

*Deputy Director-General, International Legal Affairs Bureau, Ministry of Foreign Affairs, Japan. The views expressed here are not representing the official position of the Government of Japan.

1. Basic concept of due diligence

"Every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States" , or "a duty to protect other States[1] against injurious acts by individuals from within its jurisdiction"[2], exists as a general obligation or principle emanating from the territorial sovereignty.[3] On the other hand, this obligation requires clarification in particular contexts, and other relevant rules of international law should be taken into account in the clarification.

The UNGGE Reports have indicated various measures to be taken for the prevention and mitigation of cyberattacks. Such measures include not only the measures taken inside the territories of States but also measures to cooperate in the information sharing and investigation with other States, including potential victims. Paragraph 13(c) of the 2015 UNGGE report has been most frequently associated with the due diligence obligation, but other paragraphs relating to cooperation are also relevant to the prevention and mitigation of cyberattacks.[4] Due diligence, at least in the context of the prevention and mitigation of cyberattacks, should be understood as overlapping with the duty to cooperate with relevant States. The duty to cooperate has been recognized as a basic duty of States. Friendly Relations Declarations (1970) reads:

> "States have the duty to co-operate with one another, irrespective of the differences in their political, economic and social systems, in the various spheres of international relations, in order to maintain international peace and security and to promote international economic stability and progress,

1 Corfu Channel case (UK v Albania) (Merits)(1949) ICJ Rep 1949, p22
2 Trail Smelter case (United States v Canada)(1941) Vol III RIAA 1905, p 1963
3 Island of Palmas case (Netherlands v USA) (1928) Vol II RIAA 839 (Territorial sovereignty…has as corollary a duty: the obligation to protect within the territory the rights of other State…)
4 UNGGE Report 2015 (A/70/174) para 13(a)-(h), 17(a)-(e), 28(a)-(e).

> the general welfare of nations and international co-operation free from discrimination based on such differences."[5]

While there has been no consensus on the nature of the due diligence obligation applicable to cyberattacks, UN Member States have agreed on the applicability of existing international law to cyberspace. States should discuss what constitutes the core content of the due diligence obligation arising from their territorial sovereignty, taking the duty to cooperate among States also into account.

2. Seriousness

As the Alabama Arbitral Award pointed out, due diligence obligation ought to be exercised in proportion to the risk.[6] The Trail Smelter Arbitral Award said:[7] "no State has the right to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another or the properties or persons therein, when the case is of serious consequence and the injury is established by clear and convincing evidence." The Tribunal limited the scope of obligation to the cases of serious consequence. This understanding was later confirmed by ICJ in the Pulp Mills judgment.[8]

Article 1 of the ILC Articles on Prevention of Transboundary Harm from Hazardous Activities (2001) also limited its scope to "activities not prohibited by international law which involve a risk of causing significant transboundary harm through their physical consequences." The definition of transboundary harm under the Articles itself does not necessarily exclude the harm caused by cyberattacks, but the commentary seems to limit its scope to environmental harm[9]. Articles 3 and 4 provide for the obligation to prevent and cooperate.

5 GA RES 25/2625(1970) (Declarations on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations)
6 Alabama case (USA v GB) (1872) Vol XXIX RIAA 129
7 Trail Smelter case (United States v Canada)(1941) Vol III RIAA 1905, p 1965
8 Pulp Mills case (Argentine v Uruguay) (2010) para 101
9 Article 2(c) ("Transboundary harm" means harm caused in the territory of or in other places under the jurisdiction or control of a State other than the State of origin, whether or not the States concerned share a common border)

Under the Draft Articles the seriousness is measured by the harm to persons, property or the environment[10]. In the cases of cyberattacks, what characteristics should we consider in measuring their seriousness? UNGGE reports have often emphasized the importance of the protection of critical infrastructure and the protection of human rights[11]. In measuring seriousness of cyberattacks in relation to the rights of other States, the impact on the critical infrastructures and fundamental human rights in other States should be taken into account.

3. Capacity to influence

Article I of the Genocide Convention provides for the obligation to prevent genocide. The ICJ interpreted this obligation in the Bosnian Genocide case.[12] This judgment clarifies that the obligation under Article I depends upon "the capacity to influence effectively the action of persons likely to commit, or already committing, genocide" and that this capacity "depends, among other things, on the geographical distance of the State concerned from the scene of the events, and on the strength of the political links, as well as links of all other kinds, between the authorities of that State and the main actors in the events". This part of the judgment seems to serve as a useful guidance in understanding the nature of the due diligence obligation.

ILC Draft Articles for State Responsibility provides for rules on attribution to State[13] , but, as perpetrators of cyberattacks use many layers of proxies and aliases to hide their real identity, victim States tend to face serious difficulty in proving the attribution in accordance with the provisions of the Draft Articles. States may have difficulty in accepting a broad obligation to prevent serious cyberattacks emanating from their territories in general, but, in view of the basic principle of due diligence and duty to cooperate among States, it would be useful for States to agree on the existence of responsibility of States commensurate to the

10 Article 2(b) ("Harm" means harm caused to persons, property or the environment)
11 For example, UNGGE Report 2015 para 13(f)(g)(h) and 17(c) refer to critical infrastructure and para 13(e) and 28(b) refer to human rights.
12 Bosnian Genocide case (Bosnia and Herzegovina v Serbia and Montenegro) para 430
13 ILC Articles on State Responsibility, Articles 4, 5 and 8.

capacity to influence the perpetrators of cyberattacks, even when it does not amount to the instruction, direction or control under Article 8 of the Draft Articles[14]. As an example of the responsibility arising from the capacity to influence, the Zafiro Arbitral Award admitted the responsibility of United States for the looting in Manila against British citizens by the Chinese employee, who were not under the control of its Navy at the time. The Tribunal found that there were "circumstances calling for diligence on the part of those in charge of the Chinese crew to see to it that they were under control when they went ashore"[15]. States must maintain vigilance over the activities of their institutions, officials, employees and contractors, commensurate to their capacity to influence, even when their activities are not legally attributed to States.

4. Duty to cooperate

As mentioned above, the 2015 UNGGE Report refers to several cooperative measures to be taken, including information sharing and investigation. As an example of legal instruments providing for more sophisticated mechanisms for the surveillance and notification by territorial States, International Health Regulations (IHR) (2005) provides for detailed rules concerning surveillance and notification[16]. For example, Article 6 provides: "Each State Party shall notify WHO, by the most efficient means of communication available, by way of the National IHR Focal Point, and within 24 hours of assessment of public health information, of all events which may constitute a public health emergency of international concern within its territory in accordance with the decision instrument, as well as any health measure implemented

14 Responsibilities and Obligations of States with respect to Activities in the Area (Advisory Opinion of 1 February 2011) (ITLOS) para 112 (The expression "to ensure" is often used in international legal instruments to refer to obligations in respect of which, while it is not considered reasonable to make a State liable for each and every violation committed by persons under its jurisdiction, it is equally not considered satisfactory to rely on mere application of the principle that the conduct of private persons or entities is not attributable to the State under international law (see ILC Articles on State Responsibility, Commentary to article 8, paragraph 1).)

15 Zafiro Arbitral Award (UK v US) (1925) Vol VI RIAA 160-165 (The nature of the crew, the absence of a régime of civil or military control ashore, and the situation of the neutral property, were circumstances calling for diligence on the part of those in charge of the Chinese crew to see to it that they were under control when they went ashore in a body).

16 IHR (2005) Article 5-7.

in response to those events." This 24 hours rule cannot be regarded as an obligation under customary international law, but it can be seen as a rule developed on the basis of the principles of due diligence and duty to cooperate among States. As an example of the duty to inquire into incidents caused by nationals to foreign nationals, Article 94 of UNCLOS provides for the flag State's obligation to inquire into marine casualty or incident of navigation involving a ship flying its flag and causing loss of life or serious injury to nationals of another State or serious damage to ships or installations of another State or to the marine environment.

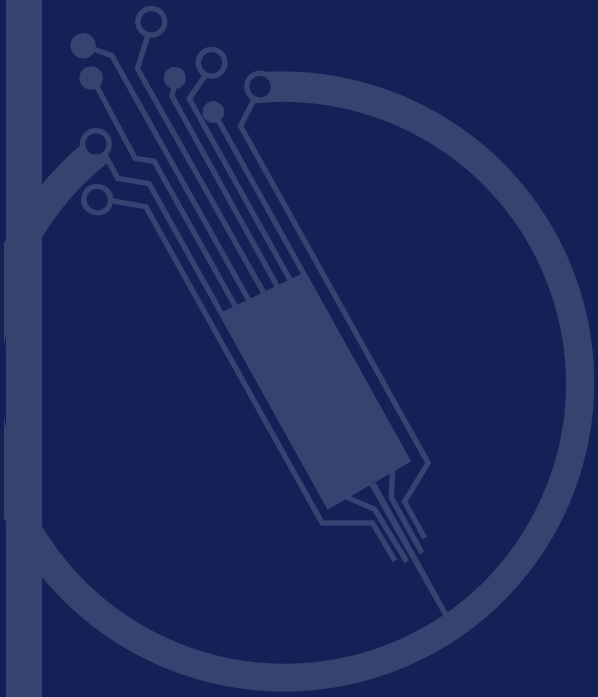
In order to prevent and mitigate cyberattacks it seems essential to inquire and investigate into potential risks of malicious cyber activities and share information about potential perpetrators and their methods, including the features of their malwares and the vulnerabilities they intend to exploit. In this regard, paragraph 13(a) and (j) of the 2015 UNGGE report refers to the cooperation in "developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security" and "responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure". Paragraph 17(e) also refers to the cooperation "in a manner consistent with national and international law, with requests from other States in investigating ICT-related crime or the use of ICTs for terrorist purposes or to mitigate malicious ICT activity emanating from their territory".
They are not referred to as legal obligation in this report, but they can be seen as having a root in the core legal principles relating to the notification and investigation arising from the basic principle of due diligence and duty to cooperate among States.

5. Core principles

Based on the forgoing, the following two points should be agreed as the core principles of due diligence and duty to cooperate among States for the prevention and mitigation of serious cyberattacks:

a. States have the obligation to take measures to prevent and mitigate malicious cyber activities causing serious damage to critical infrastructure or serious violation of human rights in other States proportionate to their capacity to influence potential perpetrators and also to the seriousness of the risk.

b. States have the duty to notify relevant State of a serious risk of threat to the latter's critical infrastructure and fundamental human rights of the latter's nationals posed by malicious cyber activities emanating from the former's territories and to inquire into such a risk of which the former have become aware.



2 The Oxford Statement on International Law Protections of the Healthcare Sector During Covid-19: Safeguarding Vaccine Research

Published 11 August 2020
106 Signatories

As the COVID-19 crisis continues to affect millions of individuals around the world, the development of a vaccine becomes an essential component of States' responses to the pandemic. A vaccine may not only save lives but also mitigate the socio-economic impact of the disease by allowing individuals to interact and work more safely.

Noting that, whilst the coronavirus pandemic and its consequences unfold, medical and research facilities in several countries have been targeted by malicious cyber operations, and that seemingly minor intrusions can disrupt or harm the availability or integrity of the data which could, among other things, compromise the ability to conclude clinical trials, obtain approval for them or manufacture or distribute an eventual vaccine,

Further noting that, because scientific development is now highly dependent on information and communications technologies spread across the globe, such harmful cyber activity may undermine States' and global efforts to contain and recover from the COVID-19 pandemic and its side-effects, Bearing in mind that COVID-19 is a highly contagious disease that respects no national borders, making international solidarity essential to restoring global health security,

Considering that the discovery and widespread provision of a safe and effective COVID-19 vaccine could save not just lives, but also economic livelihoods around the world,

Noting the Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector conclusion that '[a]ny interference with the provision of health-care, including by cyber means, risks further loss of life as thousands continue to die every day',

And emphasizing that — even if the specific application and interpretation of international law to the technologies, knowledge and data used in the process of vaccine development require fleshing out — COVID-19 vaccine, research, manufacture, and distribution are both essential medical services and part of

States' critical infrastructure that must be protected by international law, Guided by these considerations, we agree that, currently, the following rules and principles of international law protect the research, manufacture and distribution of COVID-19 vaccine candidates against harmful cyber operations. We encourage all States to consider these rules and principles when developing national positions as well as in the relevant multilateral processes and deliberations:

1. As affirmed in the first Oxford Statement, international law applies in its entirety to cyber operations by States including those that target the healthcare sector and essential medical facilities. These facilities include vaccine research, trial, manufacture and distribution facilities, other research paths to therapies and preventative measures, together with their technologies, networks and data, particularly clinical trial results, and other research.

2. International law prohibits cyber operations by States that have significant adverse or harmful consequences for the research, trial, manufacture, and distribution of a COVID-19 vaccine, including by means that damage the content or impair the use of sensitive research data, particularly trial results, or which impose significant costs on targeted facilities in the form of repair, shutdown, or related preventive activities.

3. International humanitarian law requires that at all times parties to an armed conflict: (a) respect and protect medical facilities, transport and personnel, including those involved in COVID-19 vaccine research, trial, manufacture and distribution; (b) refrain from disrupting the functioning of COVID-19 vaccine research, trial, manufacture and distribution facilities in any way, including through cyber operations; and (c) take all feasible precautions to prevent and avoid, or at least minimize, incidental harm caused by cyber operations to those facilities, and (d) take all feasible measures to facilitate their functioning and prevent their being harmed, including by cyber operations.

4. Outside of armed conflict, international law imposes negative and positive obligations on States vis-à-vis other States and individuals that afford comprehensive protection to the research, trial, manufacture, and distribution of COVID-19 vaccine candidates.

5. States must take all feasible measures to prevent, stop and mitigate malicious cyber operations against the data or technologies used for COVID-19 vaccine research, trial, manufacture or distribution which they know or should have known emanate from their territory or jurisdiction.

6. States' positive duties to ensure civil and political rights under international law require them to protect COVID-19 vaccine research, trial, manufacture and distribution to individuals subject to their jurisdiction.

7. The fulfilment of social, cultural and economic rights under international law requires States during a pandemic: (a) to ensure the manufacture and distribution of a COVID-19 vaccine in a lawful, fair, equitable, affordable and non-discriminatory manner; and (b) to cooperate to facilitate access to the vaccine by other countries.

Image credit: John Cairns, University of Oxford

The Second Oxford Statement on International Law Protections of the Healthcare Sector During COVID-19: Safeguarding Vaccine Research

Written by Dapo Akande, Antonio Coco, Talita de Souza Dias, Duncan Hollis, Harold Hongju Koh, James O'Brien and Tsvetelina van Benthem

First published on EJIL:Talk!, Just Security and Opinio Juris

The alarming spread of the global COVID-19 pandemic—now infecting nearly 19 million and claiming more than 700,000 lives worldwide—has made it increasingly urgent to define international law protections for the health care sector against malicious cyber operations.

In May 2020, malicious cyberattacks on organizations at the frontline of the response to the COVID-19 pandemic—including the World Health Organization, medical providers, research institutes, pharmaceutical manufacturers, hospitals and hospital networks—triggered a two-day virtual workshop at the University of Oxford. That workshop—co-sponsored by the Oxford Institute for Ethics, Law and Armed Conflict (ELAC) at the Blavatnik School of Government, Microsoft, and the Government of Japan—yielded the first Oxford Statement on the International Law Protections against Cyber Operations Targeting the Health-Care Sector. More than 130 international lawyers from across the globe (including some of the field's most experienced and accomplished figures) have become signatories to this Statement. It articulated a short list of consensus protections that apply under existing international law to cyber operations targeting the healthcare sector. Its announcement sparked discussion at a May 2020 Arria-Formula meeting of the U.N. Security Council on Cyber Stability, Conflict Prevention and Capacity Building.

As the pandemic continues to unfold, vaccine research has emerged as a new, critical vulnerability. Last month, the United Kingdom, the United States (US) and Canada issued a joint advisory accusing Russian intelligence services of targeting COVID-19 vaccine development "with the intention of stealing information and intellectual property." A few days after, the US Department of Justice unsealed an indictment accusing individuals linked to China's Ministry of State Security of hacking entities working on COVID-19 treatments, tests, and vaccines. International law must protect this research from external interference to ensure that a safe, effective and universally available vaccine can reach afflicted, needy populations in the near future.

This urgency led Oxford's ELAC to host a second virtual workshop on July 31, 2020, again co-sponsored with Microsoft and the Government of Japan, to hear from vaccine researchers and information security experts about the special challenges of protecting vaccine research from cyber-intrusion. Those experts explained that cyberattacks or intrusions into ongoing Phase III clinical trial research, for example, could corrupt or tamper with the relevant data needed to establish a vaccine candidate's efficacy, leading to the trial's failure, and the loss of time and lives in the fight against COVID-19.

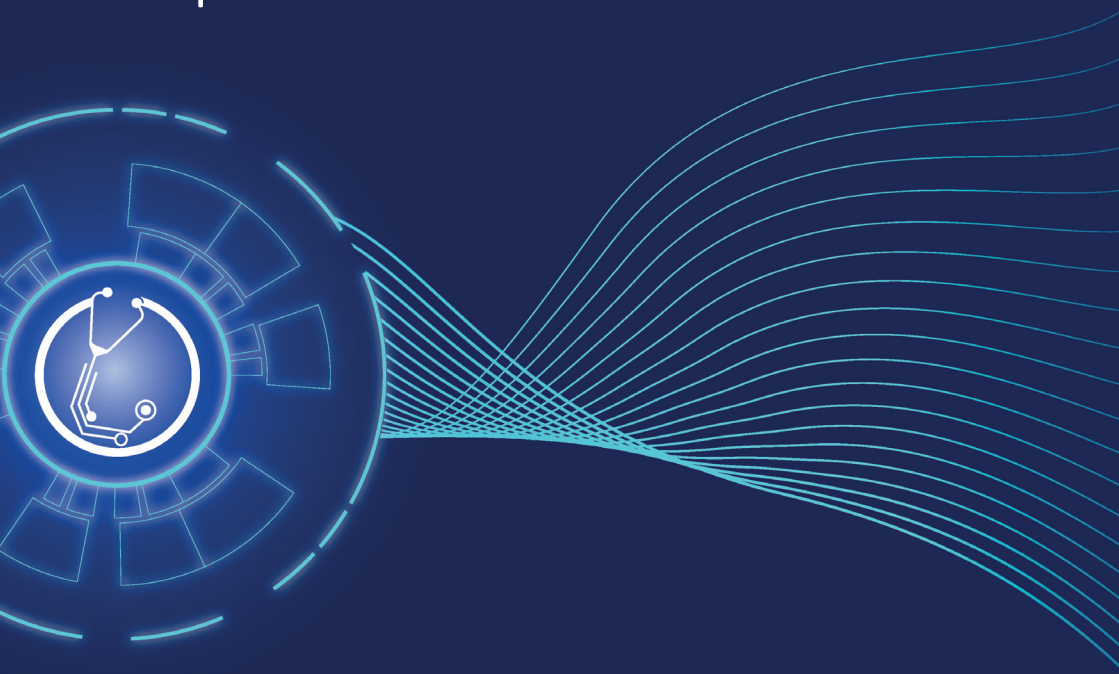
The workshop clarified both the cyber protections needed by vaccine research, and how international law applies to the protection of the development, testing, manufacture, and distribution of a COVID-19 vaccine. That discussion has now led to The Second Oxford Statement on International Law Protections of the Healthcare Sector During Covid-19: Safeguarding Vaccine Research, reproduced below.

Once again, the aim of the Second Oxford Statement is not to cover all applicable principles of international law but, rather, to articulate a short list of consensus protections that apply under existing international law to malicious cyber operations targeting vital vaccines. The Oxford Statement was opened, and remains open, for signature by international

law scholars, with hopes that it will spur discussion and clarification of the international legal framework in this area. It is part of an ongoing "Oxford Process", which aims to articulate points of consensus on international legal rules with respect to urgent global problems, ranging from cyberattacks on the healthcare sector to election security.

Global crises create unique opportunities for international lawmaking. There is no better moment to make explicit and unambiguous—in real and virtual space, in times of war and peace—that when a global pandemic rages, international law must protect the means to ending it. Why does international law exist, if not to save innocent people from needless death?

Virtual workshop
Report



The Oxford Process on International Law Protections in Cyberspace:

Safeguarding the Covid-19 vaccine research

31 July 2020

Executive Summary & Key Takeaways

On July 31st, 2020, the Oxford Institute for Ethics, Law and Armed Conflict (ELAC) held a virtual workshop, sponsored by Microsoft, on the international legal rules that protect vaccine research.

This workshop was part of the Oxford Process on International Law Protections in Cyberspace, an initiative seeking to identify points of consensus on international legal rules and principles in their application to specific sectors, objects and activities. This workshop was the second one in the Oxford Process series, following on from a workshop on the protection of the healthcare sector (May 2020).

Cyber operations targeting institutions engaged in vaccine research started almost as soon as the research itself. These operations exposed vulnerabilities in the networks of research institutions and served as a stark reminder of the importance of protecting the development of a vaccine.

During the workshop, the protection of vaccine research was reviewed through an array of disciplines: from cybersecurity through policy to law. This combination of perspectives painted a detailed picture of the threat landscape and the types of harm that cyber operations may cause. The following points emerged from the discussion:

1. Cyber operations against vaccine research present complex challenges. Even operations that do not seek the disruption or destruction of systems and/or data can damage the integrity of vaccine trials, thus slowing down the approval, production and distribution of the vaccine.

2. International law is an essential component of the toolkit that states and other actors can use to deter harmful behaviour. Its applicability to information and communications technologies (ICTs) was a point of agreement among participants.

3. For international law to fulfil its purpose, how it applies to cyber operations against vaccine research should be clarified. This would involve a process of specification of the relevant international legal rules.

4. International law already contains a range of relevant and applicable binding legal rules that constrain the behaviour of States and other actors and require the taking of positive steps to protect vaccine research.

5. The contours of many rules of international law remain pixelated. More work is needed on the meaning of 'harm', the existence of an element of intentionality in particular rules, and the types of measures through which obligations with a due diligence standard can be discharged, among others.

Background

As the fight against Covid-19 continues in hospitals, public and private health institutions, laboratories and research facilities around the world, so do cyber operations targeting or disrupting these efforts. In this context, the Oxford Institute for Ethics, Law and Armed Conflict (ELAC), co-sponsored by the Government of Japan and Microsoft, hosted a virtual workshop in May 2020 to discuss States' obligations to refrain from cyber operations against the healthcare sector and to protect it from a range of online harms. Those discussions resulted in the Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Healthcare Sector, signed by 150 international lawyers and cited as a model of how international law applies in cyberspace during the 2020 UN

Security Council Arria-Formula meeting on the issue.
This second virtual workshop, convened by ELAC with the sponsorship of Microsoft, sought to give continuity to the Oxford Process on International Law Protections in Cyberspace that started in May 2020. It applied the principles set out in the Oxford Statement on Health Care to a timely case study: the protection of data, networks and other ICTs used in the search for a Covid-19 vaccine. Its aim was to provide a more granular analysis of the relevant rules of international law in their application to this particular object of protection.

Summary of Sessions

Welcome and Introductions

Professor Dapo Akande (ELAC) gave the introductory remarks, presenting the Oxford Process to the workshop participants. This Process, which combines expert discussions with specific outputs, such as the Oxford Statement on International Law Protections of the Healthcare Sector, aims to clarify the contours of responsible behaviour in cyberspace from the perspective of international law. While the first Oxford Process workshop focused on the protection of the healthcare sector more generally, the goal of the second workshop was to dive deeper into the protection of one particular area within the healthcare sector: vaccine research.

The second workshop was driven by a need for granularity in international legal protections, made particularly acute by the increase in cyber operations against institutions engaged in vaccine research. Just as with the previous session of the Oxford Process, the aim was to identify areas of consensus on existing protections under international law. These areas of consensus would then become the basis of a second Oxford Statement. Amid a raging pandemic, clarifying how international law applies to vaccine research – the activity that can free us from the grasp of the disease – was critically important. Specifically, it can serve as a pathway to bolstering the protective measures taken by states, a deterrent to potentially harmful

conduct, and a vehicle for articulating claims of violations of the law. The workshop was organised around two sessions. The first one was aimed at providing an overview of the nature of current cyber threats and the legal and policy issues involved. Four speakers addressed four different angles for assessing the current cyber climate in relation to vaccine research. Following these presentations, the second session transitioned to an open discussion among the participants.

Session I

Presentations

Graham Ingram, Chief Information Security Officer, University of Oxford

In his remarks, Mr Ingram provided an overview of the landscape of cyber threats against Oxford University's vaccine research programme, a programme which resulted in the Oxford-Astrazeneca Covid-19 vaccine. His presentation was structured around three points: first, an observation on cybersecurity and threat actors, second, an assessment of the level of cyber maturity in universities, and third, a note on the characteristics of perpetrators of cyber operations.

Mr Ingram introduced the workshop participants to the objective of Oxford University's cyber defence team: to reduce the risk of a cyber event from causing material damage to our people, our intellectual property and our institution. To attain this objective, both preventative and reactive control measures play a key role, as it is their combination that can ensure the mitigation of the likelihood of damage to University networks. Cyber effects are delivered by a combination of people, processes and technologies across the University, Colleges, private sector partners and the UK government.

Three messages were emphasised in this presentation: that even the best reactive controls cannot eliminate all risk; that most organisations lack the capacity to defend themselves against highly determined and sophisticated actors, and that a legal framework of preventative control can be beneficial in combating harmful behaviour online. Effective

protection requires buy-in from relevant actors, as well as robust enforcement mechanisms.

Universities, as open, academic institutions, do not have the foundations for high levels of cyber security. Research is usually conducted in partnership with others and requires a high degree of openness; this was once a driver for open systems, now it drives a need to match the cyber maturity of current and potential research collaborators. To improve maturity involves an appropriate consideration of confidentiality, integrity, and availability of data sets and supporting Information Communications Technology (ICT) systems. For example, during the vaccine research, confidentiality was less of a consideration as the research was always to be shared. However, integrity and availability were critically important, especially in the context of clinical trials. If any of the cyber incidents related to the COVID research had been successful in damaging the integrity of the trials data, then approvals for use of vaccine may have been delayed or the credibility of therapeutics findings questioned. If cyber security can be considered as a spectrum of maturities, universities and schools are at the other end of the scale when compared to that of governments and financial institutions. Throughout the pandemic, the university's cyber protectors had to acknowledge that the most determined actors will find their way in.

When it comes to perpetrators, the lines between state-sponsored and purely criminal activity are becoming increasingly blurred. A blend between State and non-State criminal behaviour can be observed. Attribution is not always possible. To ensure meaningful coverage, efforts should be extended towards all cyber actors and their proxies.

Douglas Wilson, Director of Legal Affairs and International Relations, GCHQ, United Kingdom (speaking in a personal capacity)

This presentation offered a reflection on the relevant international and domestic legal frameworks, as well as on the UK's approach to cyber operations impacting vaccine research.

The relationship between privacy and security was the first point addressed in the remarks. Cautioning against the temptation to think that, in an emergency, privacy and other freedoms should yield to the demands of security and safety, the speaker emphasised the importance of privacy from both a legal and a policy lens. Legally, the right to privacy can only be limited in accordance with a test of legality, legitimate aim, necessity and proportionality. From the perspective of policy, effectiveness demands that the right to privacy be observed. This is because individuals do not want a system that does not respect their rights, including their private life. What we see today is a growing influence of private actors in the setting of international standards in the field of privacy protection.

Next, the speaker addressed relevant international legal considerations. Essential questions under international law include the contours of the prohibition of intervention and in particular the meaning of 'domaine réservé' and its relation to vaccine research. Drawing on the UK's interpretation, several inquiries come to the fore. Does the development of a vaccine amount to an essential service? Does research amount to the provision of such a service? What is the legal regulation of 'clumsy spying'? And how should we look at spying that is not clumsy, and that even goes undetected? It was suggested that a way forward may be to focus on outcomes and look for illegality where operations that cause disruption and/or destruction.

Experience had played an important role in shaping the UK approach to such incidents. WannaCry, for instance, impacted the NHS in ways that exposed a range of vulnerabilities in critical national infrastructure. An important aspect of the discussion must be the reach of protection: whether it extends to researchers, providers of medical equipment (such as PPE), and other suppliers.

Moving to domestic law, the 1990 Computer Misuse Act heavily relied on consent: some considering that the consent of every single trust in

England having to be obtained to secure partnerships with the state. This is what triggered the practice of issuing directions, that is, orders under secondary legislation to facilitate cooperation between the NHS and GCHQ. A remaining question is whether existing legislation ought to be amended to provide for implied consent or whether the practice of issuing directions can be maintained.

The final part of the presentation focused on the UK approach to attribution, including its work with international partners. It was clarified that, while it is often lamented that attribution is incredibly complex and near impossible to achieve, State organs are capable of retracing the steps of cyber operations to their perpetrators. Working with partners can speed up this process. International law plays a key role, as it gives a common language for discussing substantive thresholds and evidentiary standards.

Philip Howard, Director, Programme on Democracy and Technology, Oxford

The third presentation centred on the trends in misinformation and disinformation in their relation to the emergence of Covid-19 and the vaccines under trial. An interesting development was the arrival of new actors in generating disinformation – actors that care about perceptions in the West, with their content in English and addressees: individuals living in the West. These new actors rely on the sheer volume of fake accounts, and the connections between these accounts. On the other hand, we still observe disinformation operations that adopt another method: that of creating a network of long-term characters with multiple social media accounts. These characters may start by posting about soap operas and flowers, slowly reorienting themselves to politics. This, in turn, makes them harder to catch.

Across disinformation campaigns, one can discern common messages. Democracies are weak and failing, and they are incapable of taking quick and important decisions. Democratic leaders are soft. These campaigns are also successful in linking the long-standing anti-vax campaign with the fear of Bill Gates, 5G, chips and other conspiracy theories. The package of stories is incredibly complex and has a lot of resilience to it.

The problem is particularly consequential for public understanding of science and evidence. Long-held scientific consensus on vital issues such as climate change or the vaccines is increasingly contested, heavily debated on social media and even in the mainstream news media. New technological innovations like artificial intelligence are discussed in terms that veer from the alarmist to the exuberant.

The pandemic has shown how public health depends on the availability of high-quality medical information and clear and convincing communication on topics such as vaccines. Trusted and effective communication is a vital part of the overall public health effort to combat the virus. The spread of COVID-19 depends in large part on the sum of individual decisions made by millions: will they wash their hands, wear face masks, self-isolate if showing symptoms, and take a vaccine if it becomes available? Social media is a major means of reaching these individuals. Yet we know that social media is also full of misleading rumours and false information, which can undermine public trust in official messages. Policymakers and health practitioners urgently need to develop a capacity to identify the data deficits.

Public understanding of key issues in science and technology is often limited and misinformation about basic issues in science and technology - from natural selection to global warming - abounds.

To the speaker, attribution remains a difficult question, as there is insufficient information on whether all these actors and organisations are coordinating internationally. Thinking about possible responses is difficult not only on the level of understanding the scope of relevant rules but also on that of implementation and operationalisation. One possible way to bolster protection may be to create lists of agencies, which would allow the public to evaluate information sources.

Talita Dias, Postdoctoral Research Fellow, ELAC

In her remarks, Dr Dias gave an overview of the legal rules that are relevant to the protection of vaccine research. This presentation was based on a background paper prepared by the ELAC team and the cyber due diligence project carried out at ELAC.

Two key points were addressed. First, States have at their disposal a cyber due diligence toolkit, which enables them to fulfil their international obligations to protect vaccine research. Second, a patchwork of primary rules containing a due diligence standard requires the taking of certain measures by States.

Turning to the first point, the cyber due diligence toolkit comprises measures that ought to be adopted at all stages of the development of the vaccine. All development stages are essential for the vaccine to be produced and distributed to the population, and all these stages are highly dependent on ICTs. International law is not overly prescriptive when it comes to the nature and types of protective measures, and states thus enjoy some discretion in deciding which measures are suitable and necessary for particular contexts. Flexibility here is an advantage, as it allows contextualisation. Certain measures may be required across all stages of vaccine development, one example being the establishment of a regulatory framework. Monitoring can also be construed as a measure that ought to be adopted throughout, as cyber operations against vaccine research pose a constant threat. Other measures may only be necessary at certain stages. Examples are investigations and prosecutions, which would only take place after an incident. Cooperation as a protective measure in itself might be necessary only to the extent that it helps to contain the spread of the disease.

The second point was directed at emphasising that, regardless of whether there is a general rule of due diligence under international law, there is already a set of primary rules that require the protection of vaccine research by states. These obligations overlap in some respects, as they require the taking of measures to prevent, halt and redress certain conduct and/or harm. Four categories of obligations were examined in more detail: the Corfu Channel

principle, the no-harm principle, positive duties arising under international human rights law (for instance, under the rights to life, health, property, bodily integrity), and obligations under international humanitarian law.

All obligations share certain basic features. First, all encapsulate a triangular relationship around a particular harm: protecting a victim from a source of harm. Second, they all contain a minimum knowledge requirement. Third, they are capacity-based, that is, subject to the capacity of a State to act. However, lack of capacity is not an excuse, as all states are under an obligation to ensure a baseline of protective capacity.

Session II

Open discussion

Professor Duncan Hollis, Temple University

The goal of the open discussion was, first, to allow participants to react to the presentations, and second, to start building consensus around the scope of international legal protections. Beyond agreeing on what the law is and what it should be, participants were encouraged to consider ways of making international law more practical. Six substantive strands emerged from the discussion.

First, some participants favoured the idea of declaring legal "no-fly" zones, whereby any cyber operation against particular objects and sectors, regardless of any discernible adverse effect, should be considered illegal. Under this view, intent and other subjective elements would become immaterial: any operation impacting vaccine research would automatically be classified as a violation. Such a position comes close to a strict liability regime. Some technical experts acknowledged the benefits of this approach. It was emphasised that harm can be caused even without malice. Even operations with the sole aim of espionage can do damage to vaccine research: there is a risk that the perpetrator will damage the systems of the information contained therein on the way in or on the way out.

Second, and related to the previous strand, many participants raised particular elements of international legal rules, including elements of harm, intent, the *domaine réservé* and capacity for further elaboration. It was agreed that more specificity is needed on what is understood by the term 'harm'. Given the difficulties of establishing intent, some stated their preference for a transition from an analysis of intent to one of consequences, with further work needed on the foreseeability of certain consequences. The rule of non-intervention featured prominently in the discussions, with some participants raising the public/private nature of research institutions and healthcare providers as an important distinction. Others disagreed with the relevance of this distinction, arguing that, irrespective of the nature of the institution specifically targeted, a state's response to the pandemic falls within its *domaine réservé*.

Third, a comparison was made between rules applicable in peacetime and those applicable in armed conflict, and the participants were asked to reflect on the degree of protection that international law provides along the peacetime/armed conflict axis. While some argued that the protections under the law of armed conflict should be seen as the bare minimum that must be ensured and should consequently apply in peacetime as well, others emphasised the need to keep the rules and regimes separate, since the law of armed conflict provides specific protections of medical activities that do not exist, in this specific form, in peacetime.

Fourth, some participants expressed doubt as to the approach of compartmentalising objects of protection. They considered that today, vaccine research may be on the agenda, but tomorrow, genetic engineering may be the topic on everyone's mind. Focusing on values, rather than on specific items, was proposed as an alternative.

Fifth, technical experts were asked for guidance on the amount of information necessary to keep a sufficient level of cyber awareness amongst research personnel. It was explained that this question would be difficult to answer in the abstract, as its answer would depend heavily on the type of research.

Sixth and finally, it was also queried whether certain types of espionage could actually be considered beneficial – when done with care and contributing to the speedy development of vaccines. In this sense, some participants proposed the disaggregation of confidentiality, integrity and availability, with integrity and availability taking centre stage and confidentiality receding to the status of a secondary consideration. Others disagreed, arguing that unpacking confidentiality without impacting integrity and availability may be impossible. To get past any form of protection, one must do something, and that something can cause damage. It was acknowledged that certain forms of espionage operations can affect both confidentiality and integrity, thus imperilling vaccine research. The practice of the Jenner Institute at Oxford was highlighted, as their approach of making their work as transparent and accessible as possible could help reduce the number of operations seeking to breach their cyber defences.

Concluding remarks

In his concluding remarks, Professor Harold Hongju Koh answered three questions. Why this? Why now? Why us?

Why this object of protection? As states reach the limits of non-vaccine means of containing the pandemic, the development and distribution of the vaccine become the one and only ray of hope for freeing ourselves from Covid-19.

Why now? International law has a role to play in protecting vaccine research, production and distribution. Its role is becoming increasingly critical at a time of intensifying cyber operations against institutions engaged in the development of Covid-19 vaccines. This is why the Oxford Process can step in and produce Statements that, in a clear and concise way, outline the applicable international legal rules and how they apply to particular objects of protection.

Why us? Governments are typically slow to respond to pressing international challenges. A group of international lawyers may be best placed to provide the clarity that is so fundamental to the effective functioning of the international legal system.

List of Workshop Participants

1) Christiane Ahlborn, Legal Officer, UN Office of Legal Affairs
2) Harry Aitken, Legal Officer, International Law Branch of the Australian Department of Foreign Affairs and Trade
3) Dapo Akande, Professor of Public International Law, Co-Director, ELAC, Blavatnik School of Government, University of Oxford
4) Leonie Arendt, Consultant, Policy Branch, United Nations Office for the Coordination of Humanitarian Affairs
5) Russell Buchan, Senior Lecturer in International Law, University of Sheffield
6) Marjolein Busstra, Legal Counsel, Netherlands Ministry of Foreign Affairs
7) Scott Charney, Vice President, Security Policy, Microsoft
8) Kaja Ciglic, Senior Director, Digital Diplomacy, Microsoft
9) Antonio Coco, Lecturer in Public International Law, University of Essex and Visiting Fellow at ELAC, University of Oxford
10) Federica D'Alessandra, founding Executive Director of the Oxford Programme on International Peace and Security, Blavatnik School of Government, University of Oxford
11) Francois Delerue, Research Fellow in Cyberdefense and International Law, Institute of Strategic Research of the Military Academy, France
12) Talita Dias, Postdoctoral Research Fellow, ELAC, University of Oxford
13) Florian Egloff, Senior Researcher Cybersecurity, Center for Security Studies, ETH Zurich
14) Kristen Eichensehr, Assistant Professor of Law, UCLA Law School
15) Aude Géry, Geode
16) Berioska Morrison Gonzalez, Minister Counsellor, Permanent Mission of the Dominican Republic
17) Duncan B. Hollis, Laura H. Carnell Professor of Law, Temple University School of Law
18) Phil Howard, Director of the Oxford Internet Institute and statutory Professor of Internet Studies at Balliol College, University of Oxford
19) Zhixiong Huang, Professor of International Law & Vice Dean for International relations, Executive Director, Wuhan University Institute for Cyber Governance, Wuhan University

20) Miles Jackson, Associate Professor of Law, University of Oxford
21) Tania Jancarkova, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)
22) Jack Kenny, DPhil Candidate in Public International Law, University of Oxford
23) Harold Hongju Koh, Sterling Professor of International Law, Yale Law School
24) Masahiro Kurosaki, Associate Professor of International Law and Director of the Study of Law, Security and Military Operations, National Defense Academy of Japan
25) Henning Lahmann, Senior Researcher, Digital Society Institute, ESMT Berlin
26) Nemanja Malisevic, Director, Digital Diplomacy International Lead, Defending Democracy Program, Microsoft
27) Suzuki Masaru, First Secretary, Embassy of Japan in the United Kingdom
28) Tomohiro Mikanagi, Deputy Director-General of the International Legal Affairs Bureau, Ministry of Foreign Affairs of Japan
29) Tomáš Minárik, Head of International Organisations and Law Unit, National Cyber and Information Security Agency of the Czech Republic
30) Harriet Moynihan, Senior Research Fellow, International Law Programme, Chatham House
31) Jan Neutze, Senior Director, Digital Diplomacy, Microsoft
32) Jim O'Brien, Vice Chair, Albright Stonebridge Group
33) Michael Pinhorn, Head of Security Governance, Risk and Compliance, Information Security Team (InfoSec), University of Oxford
35) Daniela Rakhlina-Powsner, JD Candidate, Temple University
36) Przemysław Roguski, Lecturer in Law, Jagiellonian University in Kraków
37) Michael Schmitt, Professor of Public International Law, University of Reading
38) Nikhil Sud, Regulatory Affairs Specialist, Albright Stonebridge Group
39) Wieteke Theeuwen, Legal Officer, Ministry of Foreign Affairs of The Netherlands
40) Tsvetelina van Benthem, DPhil Candidate in Public International Law, University of Oxford
41) Liis Vihul, Chief Executive Officer, Cyber Law International
42) Doug W, GCHQ
43) José Singer Weisinger, Permanent Representative of the Dominican Republic to the United Nations
44) Nathalie Weizmann, Senior Legal Officer with the UN Office for the Coordination of Humanitarian Affairs

45) Briony Daley Whitworth, Assistant Director, Cyber Affairs Branch, Department of Foreign Affairs and Trade, Australia
46) Elizabeth Wilmshurst, Distinguished Fellow, International Law Programme, Chatham House
47) Robert Young, Legal Counsel, Global Affairs Canada

The Oxford COVID-19 vaccine (CHADOX1 NCOV-19)

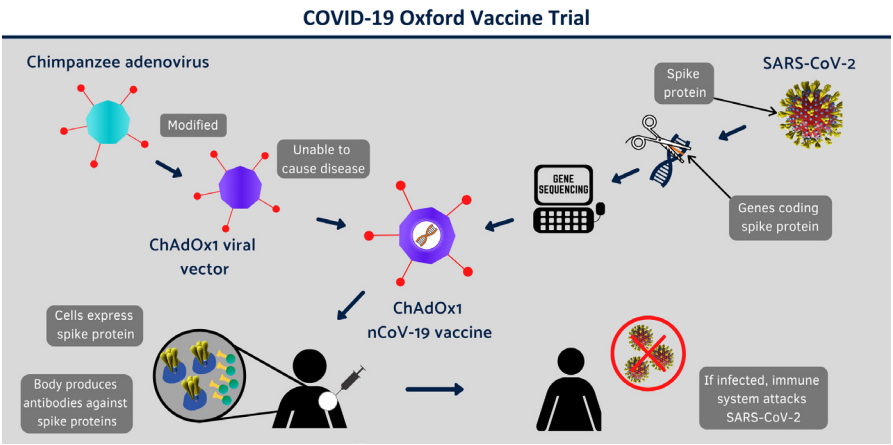
development stages and applicable protective obligations under international law

Talita de Souza Dias, Antonio Coco and Tsvetelina van Benthem

This background paper seeks to apply the interim findings of our ongoing research on 'Cyber Due Diligence' to the protection of the Oxford COVID-19 vaccine research as a case study. Our propositions are primarily grounded in protective or due diligence obligations applicable to cyberspace under international law, including, in particular, the Corfu Channel and no-harm principles, positive human rights obligations and protective duties under international humanitarian law. In what follows, we unpack these different due diligence duties and the specific measures that they may require from States to protect different stages of vaccine development. We start by setting out our key conclusions and recommendations in respect of each development stage of the Oxford COVID-19 vaccine (ChAdOx1 nCoV-19) based on information publicly available. We then delve deeper into the applicable legal framework and the extent to which we believe it covers this case study.

A broader analysis of cyber due diligence measures applicable in the context of a public health crisis can be found in A. Coco and T. de Souza Dias, 'Cyber Due Diligence in Public Health Crises', in C. Ferstman, A. Fagan (eds.), 'Covid-19, Law and Human Rights: Essex Dialogues' (University of Essex, 2020), at 297-307. For a discussion of due diligence obligations to prevent, halt and redress the spread of COVID-19 more generally, please refer to A. Coco and T. de Souza Dias, 'Prevent, Respond, Cooperate: States' Due Diligence Duties vis-à-vis the COVID-19 Pandemic', (2020) Journal of International Humanitarian Legal Studies.

1. Exploratory Stage (January-February 2020): Drug design and discovery[1]



Key measures: Protection of digital and physical resources, including data, networks, vaccine technology and biological/chemical components

States must protect the physical and digital resources, including in particular data, information and communications technologies and network infrastructures (ICTs), used for COVID-19 research conducted in their territory or under their jurisdiction, or destined for other States, in accordance with the Corfu Channel and no-harm principles as well as positive human rights obligations under international law. They may do so by adopting the necessary and appropriate legal and regulatory framework, increasing network monitoring and security, disseminating available information on threats, detection and mitigation to relevant stakeholders,[2] as well as investigating and prosecuting those responsible.

States may be required under international law to share with other States reasonable amounts of information, technology and/or data acquired by their organs or private entities incorporated in their territory during the exploratory stage of the vaccine research to an extent that

1 See 'UN Talk – Professor Sarah Gilbert', COVID-19 Oxford Vaccine Trial News, 2 June 2020.
2 See, e.g., UK National Cyber Security Centre, 'Advisory: APT29 targets COVID-19 vaccine development', 16 July 2020.

might enable or facilitate the development of a COVID-19 vaccine in other States. States must do so to the best of their abilities and to the extent that this contributes to prevent, halt and redress the contagion and spread of COVID-19 from or through their territories, in accordance with the Corfu Channel and no-harm principles, as well as their duty to protect, inter alia, the rights to life, health and work.

2. Pre-clinical Stage (March-July 2020): Testing on animal subjects - rhesus macaque

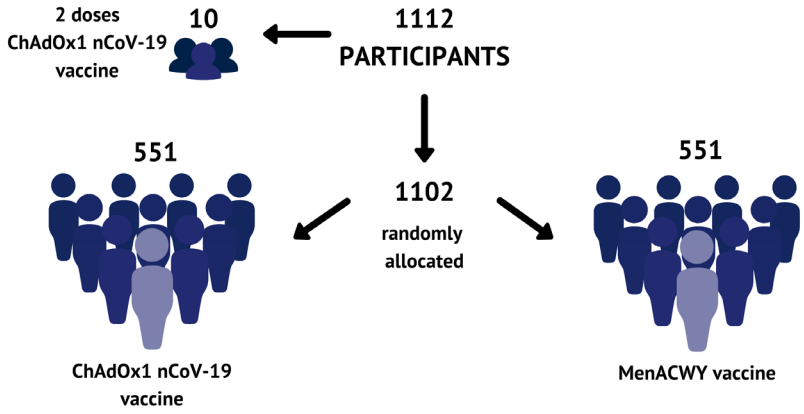
Key measures: Protection of animal testing sites, laboratories, research data and technologies

States must protect the physical sites, data and ICTs used during the pre-clinical trial stages of COVID-19 vaccine development. They must do so to the extent feasible in the circumstances to enable seamless research progress and development of a vaccine that may halt the spread of COVID-19 and prevent further outbreaks. To fulfil this duty, grounded in, inter alia, the rights to life, health and work under international human rights law, as well as the no-harm and Corfu Channel principles, States may be required to adopt relevant legislative or regulatory frameworks on biosecurity, cybersecurity and data protection, alongside enforcement measures, such as increased cyber monitoring of relevant networks, dissemination of relevant security information to employees and other users, enhanced employee screening processes, establishment of computer response emergency teams, and investigation and prosecution of those responsible for cyber harm.

3. Clinical Trials

Key measures: Protection of patient information, research data and international cooperation.

i. Phase I (April 2020): small groups of volunteers receive the vaccine to ensure it is safe (510 volunteers aged between 18-55, half with the new COVID-19 vaccine and half with a control vaccine)



ii. Phase II (April 2020): the effectiveness of the vaccine is determined with a larger group of volunteers (the maximum age of trial participants is extended to 55-70 years, then to over 70)

iii. Phase III: an even larger group of volunteers receives the vaccine, which tests the effectiveness and safety of the vaccine on a diverse group of people of different ages and backgrounds (5000 volunteers aged over 18 years, half of which receive the COVID-19 vaccine; clear efficacy endpoints will be used to assess the effectiveness of the vaccine, and volunteers from phase I and II will be included in the follow-up).

a. UK (June 2020)
b. Brazil (20 June 2020)
c. South Africa (23 June 2020)

In accordance with the right to privacy under international human rights law, States must protect confidential patient information, including

when acquired from third States or their nationals, and ranging from personal and medical information, patient questionnaires and journals. This can be done by, inter alia, adopting an appropriate legislative and regulatory framework, increasing vigilance of the networks and systems used for communication, storage and distribution of data, disseminating advice on prevention, mitigation and response to cyber threats, establishing or tasking computer emergency response teams with the responsibility to respond to malicious cyber operations, investigating and prosecuting those responsible for such operations.

To ensure the integrity of the COVID-19 vaccine clinical trial research as well as the safety, efficacy and availability of the vaccine, States must protect the life and health of trial subjects, including when those are located outside of their territory, by, inter alia, conducting appropriate medical tests and monitoring, including remotely if necessary. In accordance with, inter alia, the rights to life, health and work under international human rights law, the no-harm and Corfu Channel principles, States must also continuously safeguard the data used in and yielded by clinical trials, including, in particular, information on placebo and vaccine recipients, trial statistics and results, such as by strengthening the monitoring and resilience of digital repositories and networks, as well as medical equipment and sites, including those operated by internet-of-things systems.

States must also cooperate in gathering, coordinating and safeguarding trial data and results, including when this is done remotely, and especially when they have previously entered into specific agreements or partnerships with other States. They may do so to the extent feasible in the circumstances and in accordance with the no-harm and Corfu Channel principles and international human rights law, particularly the rights to life and health. They may do so by, inter alia, ensuring the encryption of their communications and monitoring their networks, as well as tasking computer emergency response teams with responding to cybersecurity threats, investigating and prosecuting those responsible for malicious cyber operations.

4. Release of the clinical trials' data (August 2020)

Key measures: Data protection and international cooperation

The release of statistical and other data supporting the results of COVID-19 vaccine clinical trials is a turning point in the vaccine research process, as it will conclusively establish its efficacy in generating immunity for the disease and enable its distribution to the population at large.[3] While the rights to life and health require that at least some of this information remains in the public domain to ensure transparency and accountability of the vaccination process, the integrity of clinical trials' results must be preserved to safeguard precisely the same rights. Likewise, sensitive patient data must remain confidential, in line with the right to privacy under international law. States must also share non-confidential information on clinical trials' data with other States to the best of their abilities and to the extent that this can contribute to containing the spread of COVID-19 and preventing new outbreaks within and outside of their territory.

5. Manufacturing (September 2020): 30 million experimental doses will be produced by AstraZeneca

Key measures: Efficient manufacture, protection of essential data, systems and networks

States with the capacity to manufacture the vaccine must do so promptly and efficiently, including by concluding agreements with private companies, at the very least when the clinical trial results demonstrate the safety and efficacy of the COVID-19 vaccine candidate. This is necessary to safeguard, inter alia, the rights to life of individuals under their jurisdiction and the rights to health and work of populations which they can reasonably protect. The large- scale manufacture of the vaccine is essential for its subsequent distribution to

3 'The Oxford Vaccine Centre COVID-19 Phase II/III Clinical Trial Explained', COVID-19 Oxford Trial News, 22 May 2020.

affected populations, and, to the extent that it contributes to halt and prevent the spread of COVID- 19, it may also be required by the no-harm and Corfu Channel principles.

States must also protect public and private bodies tasked with manufacturing the COVID-19 vaccine, including their intellectual property rights, data, systems, networks, technologies and manufacturing sites. They may do so by, inter alia, adopting the necessary legal and/or regulatory framework, placing security forces at the disposal of manufacturers, increasing network monitoring and resilience, disseminating information on cyber threats, tasking computer emergency response teams with responding to cybersecurity incidents, and investigating and prosecuting those responsible.

6. First Batch of Distribution (October 2020) (Europe): Should the vaccine be proven effective and safe, initial distribution of around 30 million doses can be made by September in the UK.

Key measures: Fair, equitable, affordable and non-discriminatory distribution, international cooperation, and protection of patients and health facilities

Once a COVID-19 vaccine candidate is proven safe and effective and is manufactured, States must ensure that it is distributed in a fair, equitable, affordable and non- discriminatory manner within their territory and jurisdiction, in accordance with their duty to protect the rights to life and health under international human rights law. Jurisdiction over the right to life and other civil and political rights implicated may extend to the territory of other States, provided that the duty-bearer has control over the enjoyment of those rights.[4] Although the right to health and other social, economic and cultural rights are not in principle subject to a jurisdictional trigger, States' obligations to

4 Human Rights Committee, General comment No. 36 (2018) on article 6 of the International Covenant on Civil and Political Rights, on the right to life, 30 October 2018, CCPR/C/GC/36, paras 18, 63. On the applicability of the right to life, see analysis below.

ensure those rights (in casu, through the distribution of a COVID-19 vaccine) only extend to their own territory and foreign populations to which they can reasonably supply the vaccine.[5]

To help prevent and contain the spread of COVID-19 within and outside of their territories, States must distribute available COVID-19 vaccines as widely as possible to their populations and cooperate with other States in doing so to the extent possible, in line with the no-harm and Corfu Channel principles.

During vaccine distribution within and outside of their territory, States must ensure the life, health and privacy of patients, including by protecting the data, networks and technologies used by relevant health and research facilities.

7. Second batch of Manufacturing and Distribution (December 2020): 400 million doses of the vaccine will be manufactured by AstraZeneca before the end of 2020.[6]

Key measures: Fair, equitable, affordable and non-discriminatory distribution, international cooperation, and protection of patients and health facilities

(Same as above)

5 CESCR General Comment No. 14: The Right to the Highest Attainable Standard of Health (Art. 12), Adopted at the Twenty-second Session of the Committee on Economic, Social and Cultural Rights, on 11 August 2000, para 39. See discussion of the applicability of the right to health below.
6 According to the Jenner Institute, although the university is advancing fast on its ongoing response to address the unprecedented challenges of COVID-19, it is working with AstraZeneca to define next steps on the supply of the vaccine widely to make it accessible around the world in an equitable manner. The agreement includes a commitment to make the vaccine available on a not-for-profit basis during the pandemic and to ensure broad and equitable access around the world. To achieve this, Oxford University and AstraZeneca are collaborating with a number of countries and multilateral organisations, including organizations in Brazil to address local needs. Brazil is a priority for the study because of the ascendant curve of the COVID-19. To date AstraZeneca has concluded agreements for at least 400 million doses and secured total manufacturing capacity for 1bn billion doses of the Oxford vaccine. ('Trial of Oxford COVID-19 vaccine starts in Brazil', COVID-19 Oxford Vaccine Trial News, 27 June 2020).

The applicable legal framework

General International Law

International law establishes a number of obligations requiring States ('duty-bearers') to protect other States or non-State entities ('beneficiaries') against harm caused by third States, non-State entities or natural events. These 'protective obligations' share common traits, in that they require the duty-bearer State to prevent, halt, or redress the harm in question, if it originates from or transits through their territory, or territory or infrastructure under their jurisdiction or control. Moreover, most of the said obligations can be described as obligations of conduct, in that they do not impose a pre-determined result, but generally require the duty-bearer to exercise 'due diligence', i.e. act to the best of their abilities in order to prevent, halt or redress the harm in question.

These protective obligations, directly or indirectly, appear to require States to protect facilities, supplies and data used in the development, manufacture and distribution of vaccines. This is so to the extent that disruption or interference with this process, including by cyber operations, may cause a range of harms to other States or their populations.

Such obligations include not only rules found in specialised international legal regimes (like those deriving from international human rights law and international humanitarian law, analysed infra), but also two rules of general application in international law, which are known as the 'Corfu Channel' principle and the 'no-harm' (or 'good neighbourliness') principle.

(a) The Corfu Channel principle

This principle gets its name from the 1949 Corfu Channel case between the UK and Albania, where the International Court of Justice (ICJ) held that 'it is every State's obligation not to allow knowingly its territory to

be used for acts contrary to the rights of other States'.[7] This particular obligation applies with respect to 'acts contrary to the rights of other States', without there necessarily being a violation of a particular rule of international law attributable to a State.[8] It imposes on States a standard of diligent behaviour, i.e. to employ their best efforts, to prevent or stop such acts.[9] It is triggered by actual or constructive knowledge that the acts in question are being or will be committed and limited by a State's capacity to act in the circumstances.[10]

The Corfu Channel principle has gained attention in the past few years, as States and scholars have used it as a model for different formulations of a purported customary rule or principle requiring States to exercise due diligence in cyberspace.[11] According to one iteration of this rule, States 'must exercise due diligence in not allowing [their] territory […] or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other states'.[12] Nonetheless, some governments have been reluctant to accept this formulation as a binding rule or principle of customary international law.[13]

7 Corfu Channel Case (United Kingdom v Albania), Merits, 9 April 1949, ICJ Reports (1949) 4, 22 (emphasis added).
8 The Tallinn Manual 2.0, going beyond the ICJ reasoning, argues that such acts are limited to internationally wrongful acts by a State, or acts committed by other entities that would have been internationally wrongful if committed by the State from where the harm originates or through which it transits. See Michael N. Schmitt, ed., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge (UK): Cambridge University Press, 2017), 39, § 34; 34, § 14, 35–36, § 21.
9 See e.g. Schmitt, 30; Karine Bannelier-Christakis, "Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?," Baltic Yearbook of International Law 14 (2014): 5; International Law Association (ILA), "Study Group on Due Diligence in International Law, Second Report," July 2016, 2.
10 Robert Kolb, "Reflections on Due Diligence Duties and Cyberspace," German Yearbook of International Law 58 (2015): 123–24; Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 44–45, §§ 7-9, at 47, §§ 16-18; Russell Buchan, "Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm," Journal of Conflict and Security Law 21, no. 3 (2016): 441–42.
11 Michael N. Schmitt, "In Defense of Due Diligence in Cyberspace," Yale Law Journal Forum 125 (2015): 68–81.
12 Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Rule 6, 30 (emphasis added).
13 Liisi Adamson, "Recommendation 13(c)," in Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary, by UN Office of Disarmament Affairs, Civil Society and Disarmament (New York: United Nations, 2017), at 55, § 12.

However, given the widespread acceptance that international law applies in its entirety to cyberspace, the Corfu Channel principle in its original formulation obliges States not to knowingly allow their territory or ICT infrastructures under their control or jurisdiction to be used by anyone for acts contrary to the rights of other States. Such rights may well be tied to the development, manufacture or distribution of a vaccine — an expression of sovereign authority and an exercise of governmental functions related to public health.

(b)The no-harm principle

The second rule of international law establishing a due diligence duty of general application is the 'no-harm' or 'good neighbourliness' principle. Although this principle has gained most prominence in the environmental context, its origins go far back to nineteenth century State-to-State disputes about the treatment of aliens abroad.[14] The rule was most clearly articulated in the 1941 Trail Smelter award, where the arbitral tribunal held that a State 'owes at all times a duty to protect other states against injurious acts by individuals from within their jurisdiction' which cause harm to the territory of another State, persons or property therein.[15] Many commentators have expressed the view that the no-harm principle applies to a range of harms committed in or through cyberspace, whether or not they are contrary to the rights of other States.[16] Thus, harms against facilities, supplies or data related to vaccine development, manufacture and distribution, including when

14 See, e.g., Alabama Claims Arbitration (USA v UK) (1872) 29 RIAA 125, 127, 129, 131-132; Wipperman Case (USA v Venezuela) (1887), reprinted in John Bassett Moore, History and Digest of the International Arbitrations to Which the United States Has Been a Party, vol. 3 (1898–1906), 3041; Neer Case (USA v Mexico) (1926) 4 RIAA 60, 61-62. See also
Trail Smelter Case (USA v Canada), (1941) 3 RIAA 1911, 1963-1965.

15 Trail Smelter Case, ibid, 1963.

16 See, e.g., Rebecca Crootof, "International Cybertorts: Expanding State Accountability in Cyberspace," Cornell Law Review, no. 3 (2018 2017): 603–4; Beatrice A. Walton, "Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law," Yale Law Journal, no. 5 (2017 2016): 1480–82; August Reinisch and Markus Beham, "Mitigating Risks: Inter-State Due Diligence Obligations in Case of Harmful Cyber-Incidents and Malicious Cyber-Activity – Obligations of the Transit State," German Yearbook of International Law 58 (2015): 104–6. See also Interim Report of the Ad-hoc Advisory Group on Cross-border Internet to the Steering Committee on the Media and New Communication Services incorporating analysis of proposals for international and multi-stakeholder cooperation on cross-border Internet, Strasbourg, December 2010, §§ 60-65.

perpetrated via cyber means, prima facie qualify as harms covered by the no-harm rule.

The principle has now consolidated as a rule of customary international law[17] embodied in the ILC's 2001 Articles on Prevention of Transboundary Harm from Hazardous Activities.[18] Article 3, in particular, acknowledges that States have a duty to 'take all appropriate measures to prevent significant transboundary harm or at any event to minimize the risk thereof.' According to the ILC, this duty applies beyond the environmental realm to any transboundary harm against persons, property or territory.[19] But unlike the rule articulated in Corfu Channel, the no-harm principle requires States to prevent transboundary harm even if caused by activities that are lawful or not contrary to the rights of other States.[20] This is an obligation of due diligence, not requiring States 'to guarantee that the harm would not occur' but 'to exert [their] best possible efforts to minimize the risk' thereof.[21] Moreover, a breach of the no-harm principle gives rise to liability to redress the harm,[22] with State responsibility arising subsequently from a failure to redress it.[23]

17 Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, ICJ GL No 95, [1996] ICJ Rep 226, para 29; Timo Koivurova, "Due Diligence," Max Planck Encyclopedia of Public International Law, February 2010, § 10, https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1034?prd=EPIL.

18 ILC, 'Draft articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries', in 'Report of the International Law Commission on the work of its fifty-third session (23 April–1 June and 2 July–10 August 2001)', UN Doc. A/56/10, at 144-170.

19 ILC, Draft articles on Prevention of Transboundary Harm (n. 18), 148-149. See also Timo Koivurova, "Due Diligence," Max Planck Encyclopedia of Public International Law, February 2010, § 10, https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1034?prd=EPIL.

20 Failure to exercise the requisite diligence leads to liability to redress the harm by compensation, once it materialises
— with international responsibility arising if the State fails to effect such redress. ILC, Draft articles on Prevention of Transboundary Harm (n. 18), 150.

21 Ibid., para 7.

22 Ibid.

23 Walton, 'Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law', Yale Law Journal (2016) 1460, at 1502.

International Human Rights Dimension

(a)The right to life

According to General Comment 36 of the Human Rights Committee, 'deprivation of life involves an intentional or otherwise foreseeable and preventable life-terminating harm or injury, caused by an act or omission'.[24] This means that States have the negative duty to refrain from engaging in conduct that might result in arbitrary deprivations of life, as well as the positive obligation to prevent 'reasonably foreseeable threats and life-threatening situations that can result in loss of life', even if such threats and situations do not result in actual loss of life.[25] Thus, the right to life entitles individuals to be free from acts and omissions that are intended or may be expected to cause their unnatural or premature death, as well as to enjoy a life with dignity.

Although the right to life does not incorporate a right to be healthy, certain aspects of access to healthcare and a healthy environment arise in the context of the right to life. To extent that individual lives often depend on medical treatment, public and private acts and omissions in respect of the healthcare sector may infringe the right to life.[26]Violations of the right to life might occur in cases where a patient's life is knowingly put in danger by denial of access to life-saving emergency treatment, or in situations of 'systematic or structural dysfunction in hospital services'.[27] Therefore, States have a positive duty to adopt the measures necessary to prevent those circumstances to the extent they are foreseeable and avoidable.[28]

24 HRC, General Comment No. 36 (2018) on Article 6 of the International Covenant on Civil and Political Rights, on the Right to Life, CCPR/C/GC/36, 30 October 2018, para 6.
25 Ibid., para 7.
26 See, e.g., Hristozov and Others v Bulgaria ECHR 2012-V 457, para 106.
27 Lopes de Sousa Fernandes v Portugal App no. 56080/13 (ECtHR, 19 December 2017), paras 191-192. On this issue, see Elizabeth Stubbins Bates, 'Article 2 ECHR's Positive Obligations–How Can Human Rights Law Inform the Protection of Health Care Personnel and Vulnerable Patients in the COVID-19 Pandemic?' (Opinio Juris, 1 April 2020) <www.opiniojuris.org/2020/04/01/covid-19-symposium-article-2-echrs-positive-obligations-how-can-human- rights-law-inform-the-protection-of-health-care-personnel-and-vulnerable-patients-in-the-covid-19-pandemic/>.
28 LCB v UK ECHR 1998-III 1 [36]; Brincat and Others v Malta Apps nos. 60908/11, 62110/11, 62129/11, 62312/11 and 62338/11 (ECtHR, 24 July 2014) [79]-[80]; cf Ximenes-Lopes v Brazil (Merits, Reparations and Costs) Inter- American Court of Human Rights Series C No 149 (4 July 2006), paras 89-90.

One potential difficulty in claiming that cyberattacks targeting vaccine development institutions have interfered with the right to life is that the causal and temporal connection between vaccine development and the loss of life may be tenuous. Nonetheless, to the extent that such acts may have a significant impact on the development of a life-saving vaccine, it is at the very least arguable that they are reasonably foreseeable threats that could result in the loss of life.

(b) The right to not be subjected to ill-treatment

The prohibition of ill-treatment protects individuals from treatment that reaches a minimum level of severity. While this threshold relative, it does imply severity on two levels – one, the severity of the wrong committed by an agent, and two, the severity of the victim's experience. Considering the suffering of many COVID-19 patients, one could argue that the second level would be satisfied where an attack delays the availability of a vaccine, thus leading to more suffering. However, as with the right to life, an issue here could be the temporal and causal distance between the attack and the suffering. This could make the inquiry into whether a 'wrong' has been committed more problematic. It is therefore unclear whether the obligations of States could be specified in a way that captures this type of connection between the wrong (an attack or omission to prevent and halt such attack) and the suffering of the patients.

(c) The right to health

The right to health, protected, inter alia, in Article 12 of the International Covenant on Economic, Social and Cultural Rights (ICESCR)[29] and Article 11 of the European Social Charter,[30] guarantees the right to a system of health protection which provides equality of opportunity for people to enjoy the highest attainable level of health.[31]

Although States are not required to ensure good health, they must take steps towards the full realisation of the right to health. The right is

29 International Covenant on Economic, Social and Cultural Rights, Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966, entry into force 3 January 1976.

30 ETS No.163.

31 See General Comment 14 (n 4).

considered to be one of progressive realisation, dependent on States' capacity to act, including available human and financial resources. To the extent that COVID-19 is a public health emergency, even when vaccine research efforts are fully or partly funded by private bodies, States may still have the power and thus obligation to regulate and administer those efforts. At a minimum, the immediately realisable steps that States must take involve the protection of vaccine development, manufacturing and distribution, including through safeguarding their essential networks and systems from malicious cyber operations.

Additionally, the right to health encompasses the right to prevention, treatment and control of diseases. This includes support for the necessary research and development, including for vaccines, new drugs and diagnostic tools,[32] and the creation of a system of urgent medical care in cases of epidemics.[33] In this area, the Committee on Economic, Social and Cultural Rights acknowledges the importance of States' individual and joint efforts to, 'inter alia, make available relevant technologies, using and improving epidemiological surveillance and data collection on a disaggregated basis, the implementation or enhancement of immunization programmes and other strategies of infectious disease control.'[34]

According to the CESCR, to comply with the right to health, States parties must not only respect the enjoyment of this right in other States but also 'prevent third parties from violating the right in other countries, if they are able to influence these third parties by way of legal or political means, in accordance with the with the Charter of the United Nations and applicable international law'.[35] Thus, 'depending on the availability

32 Office of the United Nations High Commissioner for Human Rights, Jutta Brunée and Tamar Meshel, "Teaching an Old Law New Tricks: International Environmental Law Lessons for Cyberspace Governance," German Yearbook of International Law 58 (2015): 134–35; Koivurova, "Due Diligence," §§ 16, 23, 44-45, at 8. See also See, e.g., Federal Administrative Court, Chamber IV, Viceconte, Mariela v. Estado nacional – Ministerio de Salud y Acción Social s/amparo ley 16.986, 2 June 1998, ordering the State to ensure the manufacturing of a vaccine against an endemic disease.
33 General Comment 14 (n 4), para 16.
34 Ibid.
35 Ibid., para 39.

of resources, States should facilitate access to essential health facilities, goods and services in other countries, wherever possible, and provide the necessary aid when required'.[36] This wording is in line with the elements of other due diligence obligations in international law, which might demand international cooperation but only to the extent that this is feasible in the circumstances.

Recent developments show the importance attached by States to cooperation in halting the spread of COVID-19. In a resolution adopted on July 10th, 2020, the European Parliament set out principles for its future EU health strategy, including global cooperation and affordable access to Covid-19 vaccines and treatments for all people worldwide as soon as they are available.[37] On June the 1st 2020, the World Health Organisation launched its 'Solidarity Call to Action to realize equitable global access to COVID-19 health technologies through pooling of knowledge, intellectual property and data'.[38] This initiative, supported by thirty-nine States so far, recognises that to halt the rapid transmission of the coronavirus and reverse the trend of consequential global distress is essential that 'everyone, everywhere can access the health technologies they need for COVID-19 detection, prevention, treatment and response'. Thus, it calls upon governments, researchers and other holders of knowledge, intellectual property or data to share those essential resources to 'leverage our collective efforts to advance scientific discovery, technology development and broad sharing of the benefits of scientific advancement and its applications based on the right to health'. Likewise, on July 15th, the WHO announced that 'seventy-five countries have submitted expressions of interest to protect their populations and those of other nations through joining the COVAX Facility, a mechanism designed to guarantee rapid, fair and equitable access to COVID-19 vaccines worldwide.'[39]

36 Ibid.
37 'Health threats: boosting EU readiness and crisis management', European Parliament News, 9 June 2020
38 WHO (note Error! Bookmark not defined.).
39 WHO, 'More than 150 countries engaged in COVID-19 vaccine global access facility', News Release, 15 July 2020.

(d) The right to privacy or private life

Two dimensions of the right to private life/ privacy recognised inter alia under Article 17 of the International Covenant on Civil and Political Rights, Article 8 of the European Convention on Human Rights (ECHR), and Article 11 of the American Convention on Human Rights, are of note here: the protection of physical integrity and the protection of medical data.

The first dimension refers to physical integrity, and is, in this sense, closely linked to the analysis under the right to life and the prohibition of ill-treatment. An analogy here could be drawn between the emergency of a health crisis, such as COVID-19, and the hazards of industrial activities. An arguable claim of violation of the right to privacy may arise where an environmental hazard attains a level that results in significant impairment of the ability to enjoy home, private or family life.[40] For instance, the European Court of Human Rights has considered the impact of pollution (including when originating from private entities) and the lack of appropriate resettlement measures on the part of State authorities to entail a violation under Article 8 of the ECHR.[41]

The second dimension refers to the protection of personal information, including medical data. The unauthorised access to such medical information would constitute an interference with the right to private life, and States are required to ensure practical and effective protection to exclude any possibility of unauthorised access.[42]

40 ECtHR, Lopez Ostra v Spain, Appl. no. 16798/90, Judgement of 9 December 1994, para. 51
41 Lopez Ostra (n 40), ECtHR, Fadeyeva v Russia, Application no. 55723/00, Judgment of 9 June 2005; ECtHR, Dubetska and Others v Ukraine, Application no. 30499/03, Judgment of 10 February 2011.
42 ECtHR, I. v Finland, App. No. 20511/03, 17 July 2008, §§ 35-47; ECtHR, Z. v Finland, App. No. 22009/93, 25 February 1997, § 95. See also Human Rights Council, 'The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights', 30 June 2014, A/HRC/27/37, para (noting that '[o]ther rights, such as the right to health, may also be affected by digital surveillance practices').

(e) The right to property

Cyber operations aiming to steal, destroy, corrupt or access confidential information related to vaccine development may not only violate individual privacy but also implicate the right to property. As is well-known, this right encompasses not only physical property, but also intellectual property, which is protected through patents and other proprietary rights or interests over non- tangible creations. Even when the integrity of information is not affected, attempts to steal or breach the confidentiality of COVID-19 vaccine data may disrupt efforts to develop, test and manufacture the vaccine. This might in turn undermine proprietary rights over its research data and physical components.

The main justification for patents and copyright is that, by incentivising and rewarding authors for their creations, they benefit society at large.[43] In the context of drug development, the importance of intellectual property rights lies in driving innovation in the pharmaceutical industry.[44] Without this incentive, few pharmaceutical companies would be interested in investing in the discovery and development of new drugs and medical treatments, including vaccines.

However, the right to intellectual property must be balanced against other rights and interests, including public health considerations, among which: a rapid and effective response to public health needs and crises; supply of quality medicines at affordable prices; effective competition through a multiplicity of potential suppliers; the provision for a wide range of pharmaceuticals to meet the basic health needs of the population; and equality of opportunities for countries in need, irrespective of their membership in the WTO, level of technological capacity, or lack of manufacturing capacity.[45] This is especially so in times of public health emergency such as the COVID-19 pandemic. For this reason, the Agreement on Trade-Related Aspects of Intellectual

43 Chapman, A Human Rights Perspective on Intellectual Property, Scientific Progress, and Access to the Benefits of Science.

44 'Access to Medicines', WHO Drug Information, Vol 19, No. 3, 2005, at 236-237; Lovett, 'Coronavirus: Drug giant AstraZeneca urged to make vaccine patent-free', The Independent, 2 June 2020.

45 Access to Medicines (n 44), at 236.

Property Rights (TRIPS),[46] concluded within the auspices of the World Trade Organization (WTO), when requiring States to adopt national legislation ensuring a global minimum standard for patent rights for a minimum term of 20 years from the filing date of a patent application for any invention,[47] including for a pharmaceutical product or process.[48]

Nevertheless, TRIPS also gives States some flexibility when balancing between IP rights and public health interests. It does so by giving States the right to enforce compulsory licenses in cases of national emergency or circumstances of extreme urgency. Compulsory licensing allows States to license the use of a patented invention to a third party or government agency without the consent of the patent-holder.[49] When adopting patent legislation, States can also provide for limited exceptions to the rights of a patent owner to exclude others from making, using, importing or selling an invention, considering the legitimate interests of others.[50] These exceptions must not "unreasonably conflict with the normal exploitation" of the patent, and may not "unreasonably prejudice" the patent owner's legitimate interests.[51] Importantly, the Doha Declaration, adopted to clarify certain provisions of the WTO agreements, reiterates States' right to grant compulsory licenses and the freedom to determine the grounds upon which licences are granted, their right to determine what constitutes a national emergency and circumstances of extreme urgency, and their freedom to establish the regime of exhaustion of intellectual property rights.[52]

Similar concerns over the integrity and confidentiality of intellectual property and other data also arise in the context of 'cyberespionage', which overlaps with but goes beyond the rights to property and privacy

46 Agreement on Trade-Related Aspects of Intellectual Property Rights, 15 April 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 UNTS. 299, 33 ILM 1197 (1994) (TRIPS)
47 Article 33, TRIPS.
48 Article 28, TRIPS.
49 Article 31, TRIPS.
50 Article 30, TRIPS.
51 Ibid.
52 WTO, Doha Declaration on the Trips Agreement and Public Health, WT/MIN(01)/DEC/W/2, 14 November 2001, para 5. See also Access to Medicines (n 44), at 239; WHO, 'Essential medicines and health products'.

under international human rights law. Although much controversy exists as to whether espionage per se, including by cyber means, is prohibited under international law, there is growing support for the view that certain types of data corruption and theft are or ought to be prohibited by international law. For instance, members of the G20 have affirmed that:

> 'no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors. All states in ensuring the secure use of ICTs, should respect and protect the principles of freedom from unlawful and arbitrary interference of privacy, including in the context of digital communications.'[53]

Likewise, Australia and China have agreed 'not to conduct or support cyber-enabled theft of intellectual property, trade secrets or confidential business information with the intent of obtaining competitive advantage'.[54] More broadly, France has stated that:
All cyberattacks against French digital systems or any production of effects on French territory through digital means by a State organ, a person or entity exercising public powers or persons acting upon the instructions or directions or control of a State constitute a violation of sovereignty. [55]

As mentioned earlier, to the extent that the access to, corruption or theft of information causes significant transboundary consequences or is contrary to the rights of other States, it will likely violate the no-harm or Corfu Channel principles, respectively.
In sum, whether data used for COVID-19 vaccine research is patented or consists of intellectual property, a trade secret, confidential business information or simply public health sensitive information, the access to, corruption or theft of such date might violate the right to privacy under

53 G20 Leaders' Communiqué, Antalya, Turkey, 16 November 2015, para 26.
54 Joint Statement Australia-China High-Level Security Dialogue, Sydney, 2017, available here.
55 France, Ministère des Forces Armées/Ministry of Defence, Droit International Appliqué aux Opérations dans le Cyberespace, September 2019.

international human rights law, as well as more general principles of international law, depending on circumstances.

(f) The right to work

It may also be possible to consider the linkages between vaccine research and the right to work, both in its dimension of the right to seek employment and prohibition of unfair dismissal and that of working in safe conditions.[56] This is because the lack of a vaccine or a drug treatment for COVID-19 has stopped millions of individuals from going back to work or working in safe conditions, resulting in unemployment or threats to the life and health of those who have risked going back to their place of work.

International Humanitarian Law[57]

International humanitarian law (IHL) also establishes a range of obligations, applicable during an armed conflict, which require States to (negatively) refrain from attacking and (positively) adopt measures to protect facilities, supplies and personnel involved in the research and development, manufacture and distribution of vaccines, including when these are targeted by cyberattacks.

Civilian or military infrastructures carrying out research and development, manufacture and/or distribution of vaccines — if authorized following the requirements of Art 12(2)(b-c) AP I — are entitled to the special protection owed to medical units, which parties to an armed conflict are obliged to respect and protect at all times.[58] Such protection, arguably, also extends to their data.[59] 'Medical units', according to the ICRC study on customary international humanitarian law, is an umbrella expression comprising 'establishments and other units, whether military or civilian, organised for medical purposes, be

56 See Articles 6 and 7, ICESCR; Articles 1 and 3, European Social Charter.
57 We thank Kubo Mačak for helpful suggestions and feedback on this section.
58 Cf. Art 12 AP I in conjunction with Art 8 AP I; Jean-Marie Henckaerts and Louise Doswald-Beck, Customary International Humanitarian Law (Cambridge: Cambridge University Press, 2005), Rule 28.
59 ICRC, 'International Humanitarian Law and Cyber Operations during Armed Conflicts — ICRC position paper', 28 November 2019, at 8.

they fixed or mobile, permanent or temporary' including, but not limited to 'hospitals and other similar units, blood transfusion centres, preventive medicine centres and institutes, medical depots and the medical and pharmaceutical stores of such units.'[60] It appears that units dedicated to vaccine development, trial, manufacture and distribution are in fact 'organized for medical purposes' and fall, therefore, within the provision's scope of application. This interpretation finds support in the ICRC Commentary to Art 8 AP I, suggesting that 'establishments which do not directly care for victims … but attempt to reduce the number of these by preventing diseases, are also considered to be medical units. This applies in particular to vaccination centres or other preventive medicine centres and institutes, and blood transfusion centres.[61]

One may also argue that, in times of a global pandemic for which a safe and effective vaccine is one way out of the crisis, vaccine doses and objects essential to its development, trial, manufacture and distribution may qualify for the special protection afforded to 'objects indispensable for the survival of the civilian population': these must not be attacked, destroyed, removed or rendered useless 'for the specific purpose of denying them for their sustenance value to the civilian population or to the adverse Party'.[62] Even where vaccine-related units do not meet the definition of 'medical units', lack the authorization ex Art 12(2)(b-c), or are not entitled to the special protection afforded to objects indispensable for civilians' survival, they still qualify for protection of civilians objects against attacks, including when perpetrated online. Malicious cyber operations — whether they engender kinetic effects or not — have the potential to intentionally or indiscriminately disrupt civilian infrastructure (including those related in any way to vaccines) and their provision of services essential to the civilian population.[63] Thus,

60 Customary International Humanitarian Law (n 58), Rule 28, at 95 (emphasis added).
61 1987 Commentary to Art. 8, AP I, § 376.
62 Art. 54, AP I and Art. 14, AP II. See also Rule 54, Customary International Humanitarian Law (n 58), esp. at 193, reminding how, during the negotiation of the Elements of Crimes for the International Criminal Court, medicines have been given as an example of objects which at times could be considered indispensable for the survival of civilians. See also Knut Dörmann, 'Preparatory Commission for the International Criminal Court: The Elements of War Crimes', 83 International Review of the Red Cross 2001, 461-487, at 475.
63 ICRC (n 59), at 5.

there is no question that, to the extent they are used as a means or method of warfare during armed conflict, intentional or indiscriminate cyber operations disrupting the development, trial, manufacture and distribution of COVID-19 vaccines would violate IHL.[64]

In addition to the duty to abide by the principles of distinction, proportionality and precaution when attacking military objectives, States also have protective obligations with respect to infrastructure over which they have control or jurisdiction. In particular, States must, both during armed conflict and in peacetime, behave diligently in adopting measures to protect civilians and civilian objects against the effects of violent cyberattacks.[65] Such precautionary measures are particularly important, given the co-dependency and interconnectivity between civilian infrastructures and lawful military objectives.[66] Thus, they may play a key role in preventing cyberattacks directed against military targets from spilling over onto civilian systems, including hospitals, vaccine research facilities and other critical infrastructure, within and outside any particular armed conflict.[67]

Finally, States continue to be bound by a general duty to act with due diligence to ensure that parties to an armed conflict do not violate IHL, including in cyberspace.[68] This entails an obligation to refrain from rendering assistance to those acting unlawfully and to 'exert their influence, to the degree possible, to stop violations of international humanitarian law'.[69]

64 Art. 51, AP I; Customary International Humanitarian Law (n 58), Rules 7, 9, 11-12.
65 Art. 58, AP I; Customary International Humanitarian Law (n 58), Rules 22-24.
66 AP I, Art. 52(2).
67 Laurent Gisel and Tilman Rodenhäuser, 'Cyber operations and international humanitarian law: five key points, Humanitarian Law & Policy, 28 November 2019.
68 Geneva Conventions of 1949, common Art. 1; AP I, Art. 1(1). Cf Marco Longobardo, 'The Relevance of the Concept of Due Diligence for International Humanitarian Law', 37 Wisconsin International Law Journal (2020) 44, at 57- 60; and Antal Berkes, 'The Standard of 'Due Diligence' as a Result of Interchange between the Law of Armed Conflict and General International Law', 23(3) Journal of Conflict & Security Law (2018) 433, at 442. Contra, see Verity Robson, 'The Common Approach to Article 1: The Scope of Each State's Obligation to Ensure Respect for the Geneva Conventions', 25(1) Journal of Conflict and Security Law (2020) 101
69 Cf. Customary International Humanitarian Law (n 58), Rule 144.

3 The Oxford Statement on International Law Protections Against Foreign Electoral Interference Through Digital Means

Published 28 October 2020
173 Signatories

We, the undersigned public international lawyers, have watched with growing concern reports of cyber incidents targeting electoral processes around the world, including allegations of foreign State and State-sponsored interference. We also note that the COVID-19 pandemic raises additional challenges to ensuring the integrity of such processes.

Whereas:

Two prior Oxford Statements have described the rules and principles of international law governing cyber operations that threaten two areas of pressing global importance, namely the safeguarding of the health care sector and global vaccine research;

International law protects electoral processes, and efforts to interfere, including by digital means, with a state's choice of its political leaders or other matters on which it has free choice contravene basic principles of the international order;

The Charter of the United Nations (UN) establishes sovereign equality and each state's political independence as bedrock elements of the international system; the UN General Assembly has affirmed that no state "has the right to intervene directly or indirectly, for any reason whatever, in the internal or external affairs of any other state"; and the International Court of Justice has held that every sovereign State has the right "to conduct its affairs without outside interference";

Article 25 of the International Covenant on Civil and Political Rights declares that "[e]very citizen shall have the right and the opportunity, without … unreasonable restrictions [t]o take part in the conduct of public affairs, directly or through freely chosen representatives; [t]o vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors"; electoral interference can infringe human rights protected under the

International Covenant on Civil and Political Rights, the African Charter on Human and Peoples' Rights, the American Convention on Human Rights, and the European Convention on Human Rights;

Other international instruments, such as the Paris Call for Trust and Security in Cyberspace (2018), have called on all stakeholders to "[s]trengthen their capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities";
All efforts by states and others to prevent such malign interferences should be consistent with international law;

The International Law Commission's 2001 Articles on State Responsibility establishes that a state is responsible for the conduct of its organs or officials, as well as for conduct carried out by persons or groups acting on the instructions of, or under the direction or control of, the state;

In line with the UN Guiding Principles on Business and Human Rights, online intermediaries and digital media companies should "conduct due diligence to ensure that their products, policies and practices … do not interfere with human rights", as recognised in the April 2020 Joint Declaration on Freedom of Expression and Elections in the Digital Age, adopted by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, and OAS Special Rapporteur on Freedom of Expression.

As states and other stakeholders learn more about the ways in which foreign cyber actions can adversely affect domestic electoral processes and how best to address such harms, international law can be further clarified and strengthened by state practice that becomes accepted as customary international law.
We affirm that all states are bound to act in accordance with the rules and principles identified below.

Applicability

1. International law applies to cyber operations by states, including those that have adverse consequences for the electoral processes of other states.

a. "Electoral processes" refer but are not limited to processes for selecting or electing individuals for public office, referenda, and plebiscites. These include:

i. Balloting: registering, casting, tabulating, or assuring the integrity of a ballot including voter registries, ballot security and integrity protocols, voting machines, and paper ballots;

ii. Verifying: systems used for reporting, recording, verifying and auditing votes and results of an election;

iii. Informing: public or private systems that provide an electorate with procedural information about how to participate in an electoral process, as well as substantive information, of whatever origin, related to an electoral process, including information on individuals or groups participating in electoral processes, such as candidates for elective office, political parties, or organizations.

b. Adverse consequences, in the electoral context, include actions, processes or events that intervene in the conduct of an electoral process or undermine public confidence in the official results or the process itself. These actions include but are not limited to intrusions into digital systems or networks that cast doubt on the integrity of election data, such as votes and voter registers, as well as cyber operations against individuals and entities involved in the election.

Duty to Refrain

2. A state must refrain from conducting, authorising or endorsing cyber operations that have adverse consequences for electoral processes in other states. States must refrain from, inter alia,

a. Interfering, by digital or other means, with electoral processes with respect to balloting or verifying the results of an election;

b. Conducting cyber operations that adversely impact the electorate's ability to participate in electoral processes, to obtain public, accurate and timely information thereon, or that undermine public confidence in the integrity of electoral processes.

c. Conducting operations that violate the right to privacy, freedom of expression, thought, association, and participation in electoral processes.

Duty Not to Render Assistance

3. A state must not render assistance to cyber operations that it knows will likely have adverse consequences for electoral processes in other states

Due Diligence

4. a. When a state is or should be aware of a cyber operation that emanates from its territory or infrastructure under its jurisdiction or control, and which may have adverse consequences for electoral processes abroad, that state must take all feasible measures to prevent, stop and mitigate any harms threatened or generated by the operation.

b. To discharge this obligation, states may, to the extent feasible, be required to, inter alia, investigate, prosecute or sanction those responsible, take measures to prevent or thwart operations spreading misleading or inaccurate information, and/or assist and cooperate with other states in preventing, ending, or mitigating the adverse consequences of foreign cyber operations affecting electoral processes.

c. The measures taken to discharge a state's obligations should be carried out in full compliance with other rules of international law.

Obligation to Protect Against Foreign Electoral Interference

5. States have an obligation to protect and ensure the integrity of their own electoral processes against interference by other states. To discharge this obligation, states may be required to put in place electoral security measures, such as legislation and backup systems, as well as to secure the availability of public, timely and accurate information on electoral processes. Any restrictive measures taken by states that interfere with human rights must be in accordance with applicable legal requirements, such as legitimate purpose, legality, necessity, proportionality and non-discrimination.

6. These rules and principles are without prejudice to other applicable international rules and ongoing processes.

'The Oxford Process has proven itself to be a highly constructive venue in which to make progress among international lawyers about the law applicable to cyberspace. While lawyers and academics spend much time and energy drawing distinctions and highlighting differences, the Oxford Process successfully steered participants toward identifying areas of agreement. Importantly, it fostered agreement on applications of law—identification of impermissible behavior—even while the participants in some cases retained differing views of the underlying legal theories. In doing so, the Oxford Process made real progress in solidifying expert views about international law's application to some of the thorniest real-world cybersecurity challenges, including ransomware and election interference.'

Kristen Eichensehr, Martha Lubin Karsh and Bruce A. Karsh Bicentennial Professor of Law and Director, National Security Law Center, University of Virginia School of Law

Image credit: Tiffany Tertipes, Unsplash

The Oxford Statement on International Law Protections Against Foreign Electoral Interference through Digital Means

Written by Dapo Akande, Antonio Coco, Talita de Souza Dias, Duncan Hollis, Harold Hongju Koh, James O'Brien and Tsvetelina van Benthem

First published on EJIL:Talk!, Just Security and Opinio Juris

Election insecurity constitutes a dangerous global threat. Thirteen prominent intelligence experts stated, in a brief filed in U.S. federal court, that: "Over the last several years, evidence has emerged that Moscow has launched an aggressive series of active measure campaigns to interfere in elections and destabilize politics in Montenegro, Ukraine, Moldova, France, Germany, the Netherlands, Estonia, Sweden, Austria, Italy, Poland and Hungary, to name just a few. They sought to inflame the issues of Catalonian independence and the Brexit vote in the United Kingdom." Unfortunately, this is also not just a problem with one State; other States appear to have adopted similar tactics and tools, making foreign election interference a critical threat to the world's democracies. In recent days, U.S. officials have, for example, accused Iran of posing as far-right U.S. citizen groups and sending threatening e-mails to U.S. voters about whether and how they should vote.

Less than a week before the most consequential election in its modern history, United States electoral processes remain startlingly insecure. In August 2020, the US Director of National Intelligence reported that China, Russia, and Iran have been "compromise[ing] our election infrastructure for a range of possible purposes, such as interfering with the voting process, stealing sensitive data, or calling into question the validity of election results." Last week, the US Justice Department

unveiled an indictment charging six Russian GRU intelligence officers, inter alia, with attempting interference in the 2017 French elections. But there is a limit to how far such a global problem can be remedied by domestic law.

These and related reports led to the Third Oxford Statement on International Law Protections Against Foreign Electoral Interference through Digital Means, reproduced below. This Statement is the third arising out of a series of virtual workshops held in 2020 during the global pandemic at the University of Oxford, co-sponsored by the Oxford Institute for Ethics, Law and Armed Conflict (ELAC) at the Blavatnik School of Government, Microsoft, and the Government of Japan. The initial workshop produced the first Oxford Statement on the International Law Protections against Cyber Operations Targeting the Health-Care Sector, which articulated a short list of consensus protections that apply under existing international law to cyberoperations targeting the health care sector. A second virtual workshop in July clarified the international legal protection of vaccine research, and how international law applies to the protection of the development, testing, manufacture, and distribution of a COVID-19 vaccine. Those deliberations led to The Second Oxford Statement on International Law Protections of the Healthcare Sector During Covid-19: Safeguarding Vaccine Research. More than 130 international lawyers from across the globe have become signatories to the first two Oxford Statements. The third workshop, which took place on 20 October 2020, brought together over 70 participants among international lawyers, diplomats, industry representatives and computer scientists, has yielded this 'Third Oxford Statement'.

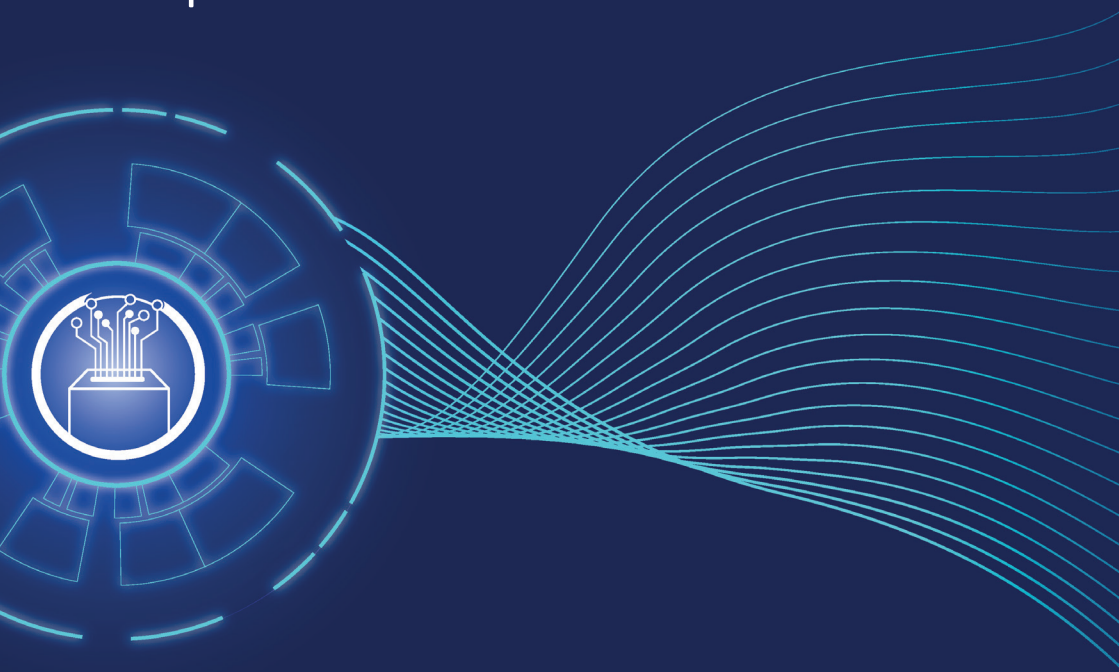
As with the prior two Oxford Statements, the goal of the present Statement is not to cover all applicable principles of international law, but rather, to articulate a short list of consensus protections that apply under existing international law to foreign cyberoperations with adverse consequences on electoral processes, such as balloting, verifying,

and providing electorates with procedural information about how to participate in an electoral process and substantive information related to that process. The Statement enumerates a range of duties of states: negative duties – to refrain from conducting cyber operations that have adverse consequences for electoral processes in other states, and not to render assistance to such operations, – as well as positive requirements of due diligence, and duties to protect and ensure the integrity of their own electoral processes from interference by other states.

Like its two predecessors, this Oxford Statement was opened, and remains open, for signature by international law scholars, with hopes that it will spur discussion and clarification about how international law applies in this area. It is part of an ongoing "Oxford Process," which recognizes that global crises create unique opportunities for agreement about the interpretation and application of international law protections, as well as their progressive development. The Oxford Process will continue to identify and articulate points of consensus on international law rules with respect to today's most urgent global problems. It is a process designed to appeal across the globe; the U.S. election may be dominating the headlines today, but foreign election interference impacts all democracies and warrants international law's continuing attention and regulation. We are pleased, moreover, to see such significant support for the Process to date, demonstrating that international lawyers can provide quick and concise guidance to States and other stakeholders on how events in cyberspace garner international legal regulation.

Use of digital means to disrupt or undermine elections and to interfere with a population's right to govern itself strikes at the very core of democracy. This Statement makes clear that international law addresses and forbids such brazen assaults on the rule of law, and states should refer explicitly to such law when speaking about election interference.

Virtual workshop
Report



The Oxford Process on International Law Protections in Cyberspace:

Protecting Elections from Foreign Cyber Interference

20 October 2020

Executive Summary & Key Takeaways

On October 20th, 2020, the Oxford Institute for Ethics, Law and Armed Conflict (ELAC) held a virtual workshop, sponsored by Microsoft, on the international legal rules that protect electoral processes from foreign digital interference. This workshop was part of the Oxford Process on International Law Protections in Cyberspace, an initiative seeking to identify points of consensus on international legal rules and principles in their application to specific objects of protection and methods employed by different cyber operations. This workshop was the third one in the Oxford Process series, following on from two workshops on the protection of the healthcare sector (May and July 2020).

Cyber operations targeting electoral processes have the capacity to sway election outcomes, erode democratic processes and shatter public trust in institutions. Harmful interferences with electoral processes have now become endemic, with foreign actors resorting to a range of sophisticated tactics for voter manipulation and suppression. In this context, the third Oxford Process workshop sought to identify the contours of applicable international legal rules that safeguard electoral processes. Technical and policy experts, government representatives and academics combined their expertise to discuss the complex questions that arise at the intersection of foreign electoral interference and the use of information and communications technologies. The following points emerged from the discussion:

1. The integrity of electoral processes is key to the functioning of democratic states. To erode democratic institutions, malicious actors have employed a range of methods that interfere with electoral processes both procedurally (in balloting, verifying and informing the public) and substantively (in seeking to sway public opinion on

substantive matters, including candidate preferences).

2. International law applies to foreign electoral interferences through digital means.

3. International legal rules matter in the context of foreign electoral interference. Far from being silent on this question, international law contains a range of international legal frameworks that regulate the planning and deployment of cyber operations impacting the conduct of electoral processes.

4. Despite a need for further specification of the contour of rules, there was widespread agreement that the core elements defining the wrong of electoral interference are the (1) tempering with a deliberative process (2) in a manipulative way.

Background

In recent years, electoral processes have become a frequent target of cyber operations. These operations have threatened the integrity of elections, attempted to influence their outcomes and undermine public confidence in democratic institutions. Without any doubt, international law protects electoral processes. The question of how and to what extent international law protects electoral processes remains, however, the subject of contestation.

To achieve more granularity in the discussion surrounding these issues, the third workshop in the Oxford Process series sought to identify the different threats affecting the conduct of elections and other democratic processes, clarify the characteristics of the cyber environment that allow or facilitate such operations, and outline the application of the existing international legal framework to the context of foreign electoral interference through digital means. This workshop

built on the two previous events hosted by ELAC and co-sponsored by Microsoft and the Government of Japan, which focused on the protection of the healthcare sector against harmful cyber operations. These two prior events resulted in two consensus documents: 1) the Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector, signed by over 150 international lawyers and cited as a model of how international law applies in cyberspace during the recent UN Security Council Arria-Formula meeting on the issue; and 2) the Second Oxford Statement on International Law Protections of the Healthcare Sector During Covid-19: Safeguarding Vaccine Research, signed by over 100 international lawyers and cited by the Acting Assistant Secretary General for the UN Office for the Coordination of Humanitarian Affairs during the August Security Council Arria-formula meeting 'Cyber Attacks Against Critical Infrastructure'.

Building on previous findings, this third workshop from the Oxford Process aimed to clarify how international rules and principles apply to electoral processes to constrain, prevent or remedy harmful conduct. The workshop was structured along two sessions, each comprising three presentations, followed by a discussion. In each session, the panellists covered a) the threats facing electoral processes, b) the applicable international legal framework, and c) the concrete measures that are being, or can be, taken to counter these digital threats and safeguard democratic processes.

Summary of Sessions

Welcome and Introduction

Professors Dapo Akande (ELAC) and Duncan Hollis (Temple University) gave the introductory remarks, presenting the Oxford Process to the workshop participants. Through expert discussions, the Oxford Process seeks to specify the application of international law to particular cyber means and objects of protection, thus identifying

areas of consensus on the scope of applicable rights and obligations in cyberspace. The Process follows four main stages: 1. Garnering consensus that norms matter in cyberspace; 2. Finding consensus that legal rules matter in regulating cyberspace; 3. Clarifying which legal rules are relevant and applicable to the context under discussion; 4. Specifying how precisely these rules apply to particular behaviours that are generally regarded as harmful. While the Oxford Process is firmly grounded in the discipline of international law and seeks to outline protections under existing law, it is also oriented towards the shaping of State behaviour. The outputs of the Process must therefore be accessible and digestible beyond academia.

What motivates the convening of Oxford Process workshops are observable trends of increased cyber activity against protected objects. Just as it was the proliferation of cyber operations against the healthcare sector that led to the first two Oxford Process workshops, it was the threat of foreign electoral interference that gave rise to the need for a third workshop focusing on the protection of democratic processes. The timing of the workshop was not coincidental – it happened a couple of weeks before the 2020 Presidential election in the United States.
In this workshop, the goal was to effectuate a transition from general statements related to the applicability of international law to specific ways in which international law protects elections and other democratic processes, such as referenda and plebiscites. Importantly, the quest for commonalities among the legal positions of experts was directed not only at prohibitions, that is – negative obligations, but also at duties to take certain measures – positive obligations – that shield protected interests from harmful conduct.

Session I

Electoral Processes and Interference with Cyber Infrastructure

Presentations

Josh Benaloh, Senior Cryptographer, Microsoft Research

The presentation offered a reflection on the particular ways of conducting elections, the vulnerabilities that accompany particular methods for conducting elections, and the pathways to ensuring resilience of democratic processes.

Starting with an overview of the experience in the United States, Dr Benaloh highlighted the decentralised nature of conducting presidential elections in the country, with over 8.000 simultaneously administered elections, each with its own rules of procedure and equipment. While heterogeneity may sometimes benefit security, the speaker opined that this system is not advantageous to the particular context of elections. When heterogeneity is the norm, all a malicious actor needs to do is to identify and target the more vulnerable jurisdictions to sway their election results. Elections are thus as strong as their weakest link.

Further, according to the speaker, the equipment market is broken due to its fragmentation, with equipment manufacturers seeking to customise for individual jurisdictions and lacking incentives to innovate. Funding is also considered scattered and erratic and, as funding is mostly local, investments in elections compete with infrastructure and other projects at the State level. Electoral systems for counting votes are thus extremely vulnerable to external interference.

Dr Benaloh raised three particular questions that impact the resilience of electoral processes.

First, the question of whether lists of voters must be public. While they are public in the United States, this is seen as a privacy issue in Europe. In his opinion, lists should be made public – the opposite makes it far too easy for malicious actors to throw in false additional voters. This, of course, raises

concerns at the intersection of election security and privacy.

Second, the question of the complexity of ballots. In the United States ballots are often so complex that there may be only one voter in a jurisdiction who casts a ballot with a particular combination of selections. This can be used to compromise voter privacy and thereby enable voter coercion – a method that has been used by the Sicilian mafia in the past. This concern does not arise with simple ballots or if anonymized ballot contents are not disclosed.

Third, the question of auditing. A trend towards the use of public audits has been observable for a long time. Traditional administrative audits typically involve going through the physical ballots, randomly selecting a set, and comparing that set to expectations. However, this type of audit relies on trust in the election administration. Within the process of public auditing, end-to-end verifiability has become a powerful tool. It can involve any voter or observer, and can detect any tampering, both internal and external. These observers can thus verify if the votes have been correctly counted. Microsoft has already built the technology to implement such end-to-end verifiability. It is open source, as it is considered a public service, and can be used for both paper and electronic ballots. While Dr Benaloh did not specifically encourage its use for Internet voting, he did note that many jurisdictions are becoming interested in Internet voting; one such example is Switzerland for its federal elections.

Marko Milanovic, Professor of Public International Law, University of Nottingham

This presentation focused on the framework of international law that applies to cyber electoral interference. While the presentation was based on a paper prepared by Professor Michael N. Schmitt which reviews questions from attribution through primary rules of international law, including non-intervention, sovereignty and human rights obligations to the response options available to an injured State, the presentation itself centred on the most controversial questions, namely

the scope of the rule of non-intervention, the nature of sovereignty, and the extraterritoriality question in international human rights law. Starting with the rule of non-intervention, Professor Milanovic emphasised that the existence of this rule is not in dispute. There is also widespread agreement on the elements of the rule: an interference in the reserved domain of a State which is coercive in character. Importantly, a State's choice as to its political system is part of this reserved domain. Thus, consensus can easily be garnered around cyber operations that directly interfere with election infrastructure and alter results by changing the vote count, as they would clearly fall foul of the rule. What remains unsettled, however, is the position of influence operations which target groups of voters, seeking to sway them in a particular direction. Examples of such operations are the disclosure of the Clinton emails, the Macron Papers or the information operations around Hunter Biden. The sharp-end question for these types of operations is whether they would qualify as coercive for the purposes of the non-intervention rule. While the law is not fully conclusive in this respect, Professor Schmitt's paper provided a list of factors that may provide a basis for considering an operation as coercive: the scale and effects of a cyber operation; its timing (to coincide with an election, for instance); whether it is deceptive; whether it exploits social vulnerabilities. According to Professor Milanovic, the crucial distinction is between operations that target a State's will ('if you do x, we will do y') and operations that target a State's ability to conduct its electoral processes. Thus, the question is less about the coercion of individual voters and more about deceptions that result in a State being coerced in such a way that it loses its ability to conduct its electoral processes.

Turning to sovereignty, a question that precedes the clarification of its elements is that of the very existence of the rule. For instance, the United Kingdom does not consider sovereignty a rule with a self-standing legal significance. While some States have affirmed its existence as a standalone rule in their national positions, many States remain silent on this issue. When it comes to its elements, a main

benefit of the rule is that it does not require proof of coercion. That said, more work is needed in determining how influence operations (rather than hacks) would be regarded under the rule.

Finally, the regime of international human rights law provides a fertile ground for discussions on interferences with electoral processes. However, the issue of extraterritorial application of human rights treaties looms large – do human rights treaties apply when a State affects the rights of individuals located outside its territory? Inevitably, according to Professor Milanovic, we will find ourselves in a world that accepts an expansive view of extraterritoriality, but we are not there yet. Professor Milanovic pointed to an important development in the area, namely the 2020 German Constitutional Court decision establishing that any surveillance operation conducted by German organs abroad would entail protections under the German Constitution. While this is a decision under German domestic law, it seems to establish the principled way of thinking about extraterritorial jurisdiction in the human rights context.

Positive obligations under international human rights law are another important component of the protection of individual rights in relation to electoral processes. These positive duties to protect a State's own population from cyber operations emanating from abroad arise under a range of rights, including the right to participate in public affairs, the right to vote, the right to privacy, the right to freedom of expression.

Allen Sutherland, Assistant Secretary, Machinery of Government and Democratic Institutions, Privy Council Office

The third presentation provided a practitioner's perspective from Canada's election in the Fall of 2019, focusing on domestic measures that can ensure the resilience of electoral systems.

At the outset, Mr Sutherland emphasised the importance of collaboration, noting that Canada is a member of the Five Eyes Intelligence Sharing Alliance, and that Global Affairs Canada has a G7

mandate for a rapid response mechanism that collaborates with other countries to identify inauthentic digital behaviour. In terms of legislative basis, Mr Sutherland referred to the Canada Election Act, which limits and constrains foreign funding and foreign advertising.
The experience and capacities of other countries, such as France, the United States, Australia and the United Kingdom have influenced the way Canada approached its 2019 election. To counter external threats, Canada knit together different capacities across government as a whole. Seven elements were considered as key to its success.

First, early preparation, including by engaging with the Cabinet on the necessary measures to safeguard elections. There is a single administrator of elections in Canada at the federal level, i.e., Elections Canada, who use paper ballots, which are considered more hack-proof. A strategic decision was made approximately 2 years prior to the 2019 election by Elections Canada to engage with the national security agencies to enhance the cyber hygiene of the organization.

Second, the use of multiple instruments: including supportive regulations, legislation and the issuing of a Cabinet directive to orient government activity.

Third, engagement with non-traditional partners both within and outside the public service. This included: the independent election commission, national security agencies, cultural organisations, and civil society as a whole. An important goal was to raise digital literacy across the population.

Fourth, the creation of a special task force to bring together cyber expertise, enforcement, diplomatic capacity, and foreign intelligence-gathering capacity. This task force – called the Security and Intelligence Threats to Elections (SITE) - funnelled information to decision-makers, thus ensuring rapid and informed responses.

Fifth, outward engagement beyond government. A document setting

out the threats to Canadian democracy was made available to the public. Direct engagement with political parties was also a critical part of the process, as political parties can be targets and potential weak links in the security of electoral processes. An investment into increasing the cyber hygiene of political parties was thus seen as paramount.

Sixth, investing in digital literacy. As noted by Mr Sutherland, an informed citizenry is the best bulwark against interference. The relevant agencies also engaged with social media platforms, and the result of this engagement can be found in the Canada Declaration on Electoral Integrity Online.

Seventh, the creation of a critical election incident public protocol, which can serve as an alarm system and prescription for action. A non-partisan panel was created to deal specifically with foreign interference. Its mandate was tightly circumscribed and only covered the election period. Its duty was to inform Canadians about threats to their right to a free and fair election and explain to them how they can avoid being influenced. An independent assessor is then tasked with reviewing the entire system, including the work of the panel. Key to the success of such a panel are the following elements: (a) having the right people who are able to react promptly and understand national security; (b) ensuring a clear mandate of the body; (c) providing access to the best information possible.

Mr Sutherland concluded his presentation by reiterating that the protection of democratic institutions requires a whole-of-government approach, direct engagement with relevant stakeholders, collaboration with external partners and the building of shared experience to counter threats to electoral processes.

Open discussion

Moderated by Professor Duncan Hollis, Temple University

The goal of the open discussion was, first, to give an opportunity to participants to react to the presentations, and second, to start building

consensus around the scope of international legal protection.

On the technical side, the participants discussed the comparative advantages of using paper and electronic ballots, as well as the different approaches to conducing elections – centralised homogenous or decentralised heterogenous systems. Regarding the type of ballots, it was emphasised that paper is a medium in elections, not necessarily a desirable property. In other words, paper ballots can be used to achieve particular goals and are often used as a proxy for verifiability. It was noted that other media can achieve the same goals, perhaps even better than paper – cloth or plastic, for example. These media are more durable than paper and inexpensive. One participant noted that while paper ballots are very labour-intensive, this very quality accomplishes a number of goals: it makes hacks difficult and creates public engagement in the election. Regarding electoral systems, according to one participant, heterogenous systems give attackers a menu of vulnerabilities that can be exploited to change election outcomes. Diversity may thus, counterintuitively, be beneficial to malicious actors. To successfully counter this threat, each and every system must be resistant and resilient.

On the legal side, the discussion branched out in five substantive directions.

A first strand concerned the duties of States regarding the conduct of electoral processes, and in particular whether, in addition to discharging any existing election-related obligations with the requisite care, States are bound, through a self-standing duty, to conduct elections in the first place. Most participants agreed that, regardless of any general obligation to conduct elections, States are bound by certain obligations in the way they organise and discharge electoral processes and interact with electoral processes in other States.

A second strand was related to international cooperation, most notably the existence of a duty to seek assistance from other States where a State lacks technical capabilities or sufficient information to respond to a threat

of digital interference. One participant noted that requesting assistance seems to belong more in voluntary norms rather than in firm *lex lata*.

The concept of critical infrastructure formed the basis of a third strand of legal discussions. It was highlighted that the use of the phrase 'critical infrastructure' may have specific implications at the domestic level, for instance enabling national security agencies to make efforts in the electoral space.

Another line of discussions focused on the distinction drawn between protection from foreign interference in electoral processes and interference that is carried out domestically, ie by a State against its own population. While all participants agreed that international law offers protection in both scenarios – both foreign and domestic interference – it was noted that the focus on foreign interference has an important messaging function, especially in the days preceding the 2020 United States presidential election.

A final fifth strand of discussions pertained to terminology, and in particular the 'adverse consequences' terminology used in the draft Oxford Statement. It was noted that the meaning of 'adverse' needs to be investigated further against the applicable legal rules, as it can be both under- and over-inclusive.

Session II

Interference in Democratic Processes and the Spread of Disinformation Presentations

Vidya Narayanan, Postdoctoral Researcher, Oxford Internet Institute

This presentation offered a reflection on the ways that computational propaganda spreads on social media, and the impact of this spread on democratic processes. Dr Narayanan based her comments on the work conducted by the Oxford Internet Institute (OII) on this question, and the impacts of propaganda observed in the 2016 United States election, as well as elections in Latin American States and India.

The focus of the presentation was junk news, and in particular the methods through which social media facilitates the spread of junk news. The preference for the term 'junk news' over 'fake news' was rationalised on the basis of the latter's use by politicians to discredit news outlets and silence the opposition. To categorise a particular news source as a 'junk news source', the researchers at OII use five criteria: (a) professionalism (professional standards, fact-checking, transparency of editorial policies); (b) style (whether it uses a sensationalist style, ad hominem attacks, emotive imagery); (c) credibility (the publishing of items that have been discredited); (d) bias (whether it is hyper-partisan, that is, whether it is characterised by a strong affiliation towards a certain type of political ideology); (e) counterfeit (whether it deliberately mimics the font and style of another more reputable news organisation).

As noted by Dr Narayanan, propaganda spreads not only through text, but also through images, videos, and memes. An observable trend is the use of discrediting tactics. In certain States, such as India and Brazil, religious content is a driver of propaganda in the electoral context. Beyond the spread of junk news on the most prominent platforms, such as Facebook and Twitter, propaganda has found a particularly fertile ground in other platforms, including WhatsApp.

More research, according to Dr Narayanan, is needed at the intersection of propaganda and generative methods (computers using advanced technology that can produce new images from existing datasets). The risk of such methods lies in the possibility of creating real images of fake persons, objects and situations that can be persuasive to audiences.

In concluding, Dr Narayanan noted the immense potential of technology and propaganda to disrupt democratic processes. Researchers do not have full access to the information kept by social media companies, and they are bound by strict research ethics, which further complicates the analysis of the means, methods and impact of digital propaganda in electoral processes.

Kate Jones, University of Oxford

The focus of this presentation was the framework of international human rights law, with a particular emphasis on the extraterritorial application of human rights treaties and the regulation of manipulation.
On extraterritorial jurisdiction, Ms Jones noted that the past twenty years have shown that the development of the law in this sphere is iterative. Today, the scope of obligations accepted to be owed extraterritorially is significantly larger than that of the past decades. The law, however, is still unsettled. A major driver for the growth of discussions on extraterritorial jurisdiction has been the possibility of accountability under international human rights law: in the domestic courts of States, regionally through courts and internationally through review mechanisms.

Substantively, there is a need to identify a threshold for condemning electoral interferences as wrongful. The collective right to self-determination may provide a fruitful way of thinking about interferences with electors as a group, rather than interferences vis-à-vis individual voters.

According to Ms Jones, the sharp-end question in this area pertains to the regulation of manipulation in politics. Disinformation, which focuses on the veracity of information, is only one type of manipulation, yet manipulation, as a term, casts a wider net than the intentional spreading of false information. Manipulation need not be only substantive: there can be manipulation of reach, as well as content. While there is no agreed definition of 'manipulation', it encompasses the 'junk news' described in the first presentation and coordinated inauthentic behaviour. Certain common elements in manipulative campaigns include the scale of manipulation, the use of fake accounts, the spread of fake content, the coordination between a network of accounts, and the lack of authenticity in identity. At its base, manipulation attempts to tamper with an audience's reasoning without the audience being aware of the manipulation. Misinformation finds itself excluded under this understanding of manipulation, as it lacks an intention to mislead.
Many rights have bearing on the regulation of manipulation: freedom

of thought and opinion, rights of political participation, freedom of expression, privacy. For all these rights, it is important to draw lines between acceptable persuasion and unacceptable manipulation. The obligations that flow from these rights both constrain States in their own operations (ie require states not to engage in certain types of operations) and require States to take certain measures to protect individuals within their jurisdiction. States should explicitly condemn manipulation. The line between legitimate and illegitimate campaigning must be clear to the relevant stakeholders. States must also take other measures, such as educating their populations on the tactics and effects of manipulation, guiding online platforms on the definitional boundaries of manipulation, and ensuring the neutrality of internet intermediaries. States must also ensure adequate accountability and access to effective remedies.

In delineating the scope of obligations under international human rights law, Ms Jones noted the importance of cultural expectations and context. She illustrated these cultural discrepancies through the different approaches to political advertising adopted in the United States and Europe.

While only States are direct duty-bearers under international human rights law, non-State actors, such as businesses, have responsibilities to respect human rights. According to Ms Jones, internet intermediaries should mainstream human rights law language in their decision-making on content moderation.

Nick Pickles, Senior Director for Public Policy, Twitter

This presentation provided an overview of how Twitter approaches the election period. As an overarching theme, it was highlighted that there is an increasing call for clearer rules but also for flexibility in their application, depending on the particular circumstances that may arise in the lead up to elections. An issue of key importance for platforms such as Twitter is proactive communication with users.

Twitter's rules are public, and they contain a specific set of rules on manipulation. Rather than focusing on content, the rules look at particular forms of behaviour, such as the high-volume use of automated accounts. The feedback received by Twitter users indicated that there is no desire for the platform to make decisions on the truth or falsity of information, but rather to give users the context that would allow them to make up their own minds. This is why Twitter started using labels that contextualise pieces of information. Additionally, there is a reporting form that allows the flagging of content. To strike the right balance in its measures, Twitter works with civil society, election authorities and enforcement agencies. The aim, ultimately, is to avoid the use of labels or content takedowns as a tool for silencing opponents, but rather to add critical context.

The context political advertising provides, according to Mr. Pickles, a perfect example of platforms being placed in the position typically designed for regulators. Twitter has prohibited political advertising globally since 2019, irrespective of who the advertiser is. It was also noted that the distinction between foreign and domestic interferences seems moot for the platform: in the particular context of the 2020 United States presidential election, false claims of victory were expected from domestic actors rather than foreign ones.
An issue of particular importance for Mr Pickles is that of communicating credible expectations to users. Twitter attempted a number of nudges addressed to users to curb the spread of manipulated information: asking users to first read the source of the information they intend to retweet or to quote content from particular tweets instead of merely retweeting them.

On the legal side, Mr Pickles urged the participants to consider the notion of sovereignty very carefully, as this principle may overcorrect and act to the detriment of the free and global internet. He further noted that the discussions should go beyond the platforms most talked about and look at less governed spaces and infrastructure providers.

Finally, he noted that a major challenge is the over-classification of information: the vast majority of real-time information sits with governments and is classified, which makes any judgment by the industry particularly difficult.

Open discussion

Moderated by Professor Dapo Akande, ELAC

The open discussion focused on five legal questions.
First, the participants debated the core of the wrong in the operations discussed: should the proscribed operations be limited to intentional manipulation, or encompass operations that, while not intentional, lead to harmful effects? One participant proposed a focus on certain means that can be presumed to be intentionally manipulative.
Some participants favoured a prohibition that would encompass any interference in the deliberative process or in the content of deliberation.

Second, the structure of online platforms was discussed, and in particular whether the business model of internet intermediaries clashes with the aim of achieving an open, free and transparent internet environment. One participant noted that other areas of law, such as anti-trust law, may be particularly relevant to the discussion of platform structures and streams of revenue. According to representatives from the private sector, the advertising business model is not, as such, incompatible with the aim of openness and transparency. What is important is to ensure interoperability between platforms, and to conceive of transparency as a way of enabling user control.

Third, some participants called for more granularity in the discussion of extraterritorial application of human rights treaties. It was highlighted that State positions on extraterritoriality evince divergences depending on the particular treaty at hand and the type of obligation at stake (negative or positive). One participant noted that there is no sound normative basis on which to deny extraterritorial application of negative human rights obligations. The sharp-end question, this participant

opined, is that of the extraterritorial scope of positive obligations.

Fourth, a number of participants argued that, as part of the positive duties under international law, States are bound to educate their population, thereby increasing their digital literacy and resilience to manipulative operations.

Fifth, another type of positive duty discussed was that of States' duties to regulate online intermediaries. One participant argued that the focus should not be on the particular type of media or intermediary, but on the character of the activity, thus suggesting a framework regulating foreign activities directed at domestic electoral processes. A number of participants noted that urging States to regulate intermediaries may result in overreach, and thus censorship.

Image credit: Unsplash

Concluding remarks

In his concluding remarks, Professor Harold Hongju Koh pointed to the importance of the timing of the workshop, taking place just two weeks before the 2020 United States presidential election. The timing was considered of particular importance since, just four years prior, the 2016 United States presidential election had become emblematic for foreign digital interference in electoral processes. Thus, a clear statement from an expert group of international lawyers that foreign interference in electoral processes is off-limits could play a powerful messaging function.

Admittedly, the topic of foreign electoral interference is complex. Despite its complexity, Professor Koh noted that the discussion clearly pointed to areas of consensus on international legal protections. While some issues of specification may linger and would benefit from further engagement, the basic contours of the applicable duties can be established in an Oxford Statement.

By issuing another statement on the international law protections against foreign electoral interference through digital means, the group of international lawyers would make its own contribution to the safeguarding of democratic processes, and once again stand on the right side of history.

List of Workshop Participants

1. Christiane Ahlborn, Legal Officer, UN Office of Legal Affairs
2. Dapo Akande, Professor of Public International Law, Co-Director, Oxford Institute for Ethics, Law & Armed Conflict (ELAC), University of Oxford
3. Mariana Salazar Albornoz, Member of the Inter-American Juridical Committee
4. Leonie Arendt, Independent Law & Policy Consultant
5. Josh Benaloh, Senior Cryptographer, Microsoft
6. Meredith Berger, Senior Manager, Defending Democracy, Microsoft
7. Russell Buchan, Senior Lecturer in International Law, University of Sheffield
8. Marjolein Busstra, Legal Counsel, Netherlands Ministry of Foreign Affairs
9. Scott Charney, Vice President, Security Policy, Microsoft
10. Kaja Ciglic, Senior Director, Digital Diplomacy, Microsoft
11. Sarah Cleveland, Louis B. Henkin Professor of Human and Constitutional Rights, Columbia Law School
12. Antonio Coco, Lecturer in Public International Law, University of Essex and Visiting Fellow at ELAC, University of Oxford
13. Gary Corn, Professor of Law and Director of Technology, Law & Security Program, American University Washington College of Law
14. Federica D'Alessandra, founding Executive Director of the Oxford Programme on International Peace and Security, Blavatnik School of Government, University of Oxford
15. Jennifer Daskal, Professor of Law and Faculty Director of Technology, Law & Security Program, American University Washington College of Law
16. François Delerue, Research Fellow in Cyberdefense and International Law, Institute of Strategic Research of the Military Academy, France
17. Talita Dias, Postdoctoral Research Fellow, ELAC, University of Oxford
18. Evelyn Douek, Lecturer on Law and S.J.D. candidate at Harvard Law School
19. Florian Egloff, Senior Researcher Cybersecurity, Center for Security Studies, ETH Zurich
20. Kristen Eichensehr, Martha Lubin Karsh and Bruce A. Karsh Bicentennial Professor of Law, University of Virginia
21. David Fidler, Adjunct Senior Fellow for Cybersecurity & Global Health, Council on Foreign Relations

22. Aude Géry, Geode
23. Geoff Gilbert, Professor of International Human Rights & Humanitarian Law, School of Law and Human Rights Centre, University of Essex
24. Elaine Gorasia, Assistant Legal Adviser, FCDO
25. Oona Hathaway, Gerard C. and Bernice Latrobe Smith Professor of International Law and Counselor to the Dean, Yale Law School
26. Duncan B. Hollis, Laura H. Carnell Professor of Law, Temple University School of Law
27. Liz Howard, Senior Counsel, Democracy Program, Brennan Center for Justice, NYU Law School
28. Alan Hu, Deputy Senior State Counsel, International Affairs Division, Attorney-General's Chambers of Singapore
29. Zhixiong Huang, Professor of International Law & Vice Dean for International relations, Executive Director, Wuhan University Institute for Cyber Governance, Wuhan University
30. Eric Talbot Jensen, Professor of Law, Brigham Young University
31. Kate Jones, University of Oxford
32. Kadri Kaska, Head of Law Branch, NATO CCDCOE
33. Chimène Keitner, Alfred & Hanna Fromm Professor of International Law, UC Hastings Law
34. Lucas Kello, Associate Professor of International Relations, University of Oxford
35. Jack Kenny, DPhil Candidate in Public International Law, University of Oxford
36. Kate Klonick, Assistant Professor of Law, St. John's University Law School
37. Harold Hongju Koh, Sterling Professor of International Law, Yale Law School
38. Elaine Korzak, Visiting Assistant Professor of Cybersecurity, Middlebury Institute of International Studies at Monterey (MIIS)
39. Leonhard Kreuzer, Research Fellow, Max Planck Institute for Comparative Public Law and International Law
40. Joanna Kulesza, Professor of Law, University of Lodz
41. Masahiro Kurosaki, Associate Professor of International Law and Director of the Study of Law, Security and Military Operations, National Defense Academy of Japan
42. Henning Lahmann, Senior Researcher, Digital Society Institute, ESMT Berlin
43. Nemanja Malisevic, Director, Digital Diplomacy International Lead, Defending

Democracy Program, Microsoft

44. Suzuki Masaru, First Secretary, Embassy of Japan in the United Kingdom
45. Tomohiro Mikanagi, Deputy Director-General of the International Legal Affairs Bureau, Ministry of Foreign Affairs of Japan
46. Marko Milanovic, Professor of Public International Law, University of Nottingham School of Law
47. Tomáš Minárik, Head of International Organisations and Law Unit, National Cyber and Information Security Agency of the Czech Republic
48. Harriet Moynihan, Senior Research Fellow, International Law Programme, Chatham House
49. Joanne N, Deputy Director International, GCHQ
50. Vidya Narayanan, Post-doctoral researcher, Computational Propaganda Project, Oxford Internet Institute
51. Jan Neutze, Senior Director, Digital Diplomacy, Microsoft
52. Naofumi Nishigori, Ministry of Foreign Affairs, Japan
53. Kazuho Norikura, Ministry of Foreign Affairs, Japan
54. Jim O'Brien, Vice Chair, Albright Stonebridge Group
55. Kate O'Sullivan, General Manager, Digital Diplomacy, Microsoft
56. Jens D. Ohlin, Vice Dean and Professor of Law, Cornell Law School
57. Patryk Pawlak, Executive Officer, European Union Institute for Security Studies
58. Nick Pickles, Senior Director for Public Policy, Twitter
59. Gowri Ramachandran, Counsel, Democracy Program, Brennan Center for Justice, NYU Law School
60. Steven Ratner, Director, Donia Human Rights Center and Bruno Simma Collegiate Professor of Law, University of Michigan Law School
61. Alix Richard, Member of the Inter-American Juridical Committee
62. Przemysław Roguski, Lecturer in Law, Jagiellonian University in Kraków
63. Corinna Seiberth, Lawyer, Federal Department of Foreign Affairs FDFA, Directorate of International Law, International Law Division, Switzerland
64. Nikhil Sud, Regulatory Affairs Specialist, Albright Stonebridge Group
65. Allen Sutherland, Assistant Secretary to the Cabinet, Machinery of Government, Privy Council Office, Canada
66. John Swords, Legal Adviser and Director of the Office of Legal Affairs at NATO Headquarters

67. Nicholas Tsagourias, Professor of International Law, University of Sheffield
68. Tsvetelina van Benthem, Research Officer, ELAC

Liis Vihul, Chief Executive Officer, Cyber Law International

Philippa Webb, Professor of Public International Law, King's College London

Robert Young, Legal Counsel, Global Affairs Canada

The content of the background paper was published in Michael N Schmitt, 'Foreign Cyber Interference in Elections' (2021) 97 International Law Studies 739.

Foreign Cyber Interference in Elections: An International Law Primer

*Michael N. Schmitt**

* Professor of International Law, University of Reading; Director of Legal Affairs, Cyber Law International.
With appreciation to Marko Milanovic and Liis Vihul for invaluable comments and suggestions on drafts of this piece.

With US elections looming, it is a propitious moment to examine the international law rules bearing on foreign interference in this fundamental expression of democracy. Sadly, little appears to have changed since the US intelligence community concluded with a "high degree of confidence" that "Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election." This August, for instance, the Director of the National Counterintelligence and Security Center warned,

> Ahead of the 2020 U.S. elections, foreign states will continue to use covert and overt influence measures in their attempts to sway U.S. voters' preferences and perspectives, shift U.S. policies, increase discord in the United States, and undermine the American people's confidence in our democratic process. They may also seek to compromise our election infrastructure for a range of possible purposes, such as interfering with the voting process, stealing sensitive data, or calling into question the validity of the election results.

And this time the finger is pointed not only at Russia, but also China and Iran. Microsoft has confirmed that actors in all three states are actively targeting the election.

While interference in American elections has captured most attention, the phenomenon is global. For instance, in 2014 CyberBerkut, a group of Russian hacktivists, targeted the Ukrainian Central Election Commission, bringing its network down for twenty hours and nearly leading to the announcement of a false winner. In 2017 the GRU (Russian military intelligence) purportedly conducted operations directed at Emmanuel Macron's campaign for the French Presidency, while the next year a distributed denial of service attack was conducted against the Russian Central Election Commission, allegedly from locations in fifteen countries.

Such election-related activities in cyberspace raise the question of their lawfulness under international law. This article examines that question from three angles. First, it assesses if and when election interference by cyber means amounts to a violation of international law. Second, it considers the duties states shoulder to put an end to hostile cyber election interference. Finally, it closes with a brief survey of response options under international law available to states that are facing such interference.

I. Election Interference as a Violation of International Law

An internationally wrongful act consists of two elements [Articles on State Responsibility (ASR), art. 2]. First, the action or omission in question must be legally attributable to a state. Second, that act must breach an obligation owed in international law to another state. I will first briefly examine the attribution element, and then move on to the various substantive obligations that election interference might breach: the prohibition of intervention, the duty to respect the sovereignty of other states, and the obligation to respect human rights.

A. Attribution

Attribution in the legal sense must be distinguished from attribution in the technical sense of the word, although the latter forms the factual predicate for the former. Legally, the concept of attribution denotes those situations in which the conduct of humans is regarded as that of a state. The clearest basis for attributing to a state a cyber operation that interferes with an election is when it is conducted by an organ of that state (ASR, art. 4), as in the Russian GRU's 2016 US election interference. When non-State actors conduct cyber operations, the most likely basis for attribution is that they acted "on the instructions of, or under the direction or control of" the state (ASR, art. 8). This would appear to be the legal basis for attribution of Internet Research Agency's 2016 operations to Russia.

Absent attribution to a state, cyber election interference by non-state actors does not violate international law, although it may trigger positive obligations of prevention that are discussed below. And even if attributable to a state, the interference must breach an obligation owed to the state conducting the election before it qualifies as an internationally wrongful act. In that regard, discussion first turns to the prohibition of intervention.

B. Prohibition of Intervention

The rule of international law that has drawn the greatest attention with respect to foreign cyber election interference is the prohibition of intervention into the internal or external affairs of other states (see Tallinn Manual, Rule 66). Appearing in such instruments as the 1970 Friendly Relations Declaration, it is a well-accepted rule of international law, the applicability of which in cyberspace was confirmed by the 2015 UN GGE report that was subsequently endorsed by the General Assembly. Variants of the rule also appear in treaties such as the Charter of the Organization of American States, although caution is merited in applying those rules because their parameters may differ from the customary rule discussed below.

As understood in customary law, intervention consists of two elements famously set forth by the International Court of Justice in its Nicaragua judgment, both of which must be satisfied before a breach exists. First, the cyber operation in question must affect another state's internal or external affairs, that is, its domaine réservé. Second, the cyber operation has to be coercive. States that have spoken to the issue are in accord as to these constitutive elements of the rule. For instance, the 2019 International Law Supplement to Australia's International Cyber Engagement Strategy explains, paraphrasing the ICJ in Nicaragua, that:

> "A prohibited intervention is one that interferes by coercive means (in the sense that they effectively deprive another state of the ability to control, decide, or govern matters of an inherently sovereign nature), either

directly or indirectly, in matters that a state is permitted by the principle of state sovereignty to decide freely" (see also, e.g., Australia, France, Netherlands, United Kingdom, United States here and here).

Within the domaine réservé, the field of activity left by international law to states to regulate, states enjoy discretion to make their own choices. Elections represent a paradigmatic example of a matter that is encompassed in the domaine réservé; in fact, the ICJ cited the "choice of political system" to illustrate the concept. That said, the increasing regulatory reach of international law is causing certain state activities to fall outside the domaine réservé, as exemplified by the expansion of international human rights law. Today, rights like the freedom of expression, the right to privacy, and the right to vote (discussed below) can be implicated by certain election-related activities. Thus, for example, a foreign state providing access to secure online communications to individuals whose right to political expression during an election is being impeded by the territorial state would not intrude into the latter's domaine réservé. The operation might violate other obligations owed to the territorial state, but not the prohibition of intervention.

While foreign election interference usually will manifestly transgress the victim state's domaine réservé, the application of the second element of prohibited intervention – coercion – to such interference is far more complicated. It also occupies center stage with respect to intervention, for, as the ICJ explained in Nicaragua, "The element of coercion… defines, and indeed forms the very essence of, prohibited intervention."

Thus, cyber operations that are coercive have to be distinguished from those that are merely influential or persuasive. Noting that "[t]he precise definition of coercion, and thus of unauthorised intervention, has not yet fully crystallised in international law," the Netherlands Ministry of Foreign Affairs has observed that "[i]n essence it means compelling a state to take a course of action (whether an act or an omission) that it would not otherwise voluntarily pursue. The goal of the intervention must be to effect change in the behaviour of the

target state." The challenge is to identify the point at which permitted influence becomes prohibited coercion.

A useful way to approach the issue is to distinguish election-related cyber activities that affect the state's ability to conduct an election from those that target voter attitudes. Foreign cyber activities that deprive a state of its ability to act vis-à-vis its domaine réservé are almost always coercive. They make it objectively impossible or substantially more difficult for the state to pursue a particular policy or activity, as when a cyber operation interferes with either the actions of state authorities administering an election or with the election infrastructure itself. The obvious example would be using cyber means to cause a miscount, which would be coercive because the real choice of the state, as reflected in the vote, is being repressed. This could be done by directly tampering with the vote count, disabling election machinery or causing it to malfunction, blocking e-voting, and the like.

Foreign states can also indirectly disrupt a state's ability to conduct an election by engaging in activities directed at voters, for example by engineering voter suppression. Consider the use of social media to falsely report that a dangerous incident, like an active shooter situation, is on-going near voting locations and that people should stay out of the area. Reasonable individuals would follow those instructions, and thus not cast their vote. Or social media could be used to give improper instructions about voting, such as the wrong location, or block or alter correct information as to where to vote. An example was the posting of tweets in 2016 in both English and Spanish to the effect that individuals could vote for Hillary Clinton through text messaging. Those who followed the instructions did not cast their vote because it is not, in fact, possible to vote via text message in the United States. Election returns even could falsely be reported prior to the polls closing, causing voters to reasonably conclude that because their candidate has already effectively lost, there is no point in going to vote. In all of these cases, the target state's ability to make free choices by means of its election

has effectively been coerced, regardless of whether it could conclusively be shown that the outcome of the election was altered.

Of course, a rule of reason should apply. Operations that result in only a very limited number of voters voting improperly or not voting at all would be unlikely to qualify as coercive. Other issues such as the timing of an operation or whether the state had an opportunity to thwart it might also weigh in the assessment. But by and large, cyber operations intended to directly or indirectly affect the state's ability to conduct an election by targeting either state-end electoral administration and infrastructure or the voters' ability to properly cast a ballot are coercive in nature.

The more difficult case is that of cyber activities intended to influence the electorate's attitudes towards a particular candidate or issue on the ballot. In these cases, information operations, although directed at voters, are being used as a means to achieve the goal of coercing the State.

While no definitive standard exists for assessing such activities against the requirement of coercion, the assessment is necessarily one of degree.

Arguably, it is reasonable to characterize as coercive those cyber operations that deprive the electorate, or a substantial number of individual voters, of information bearing on the election. After all, having access to reliable information about candidates or issues would seem essential to ensuring the election is meaningful. Examples might be denial of service attacks against a campaign's website or social media presence, or the targeting of media outlets that support a particular candidate.

A more difficult case is that in which information regarding candidates or issues is pushed to the electorate by a foreign state. This is a critical issue, for the greatest success in influencing elections has been achieved "by influencing the way voters think, rather than tampering with actual vote tallies."

Traditional messaging setting forth a state's position on a foreign election is not coercive, a conclusion supported by widespread state practice; it is designed to influence and persuade, not coerce. The unsettled question is whether there is some point at which the foreign state's information campaign becomes coercive. Imagine, for instance, a foreign state investing sufficient resources in support of a candidate to overwhelm the opponent's advertising, thereby allowing the former to dominate the traditional and social media information space. As it stands, the law is not sufficiently clear as to whether, and if so when, information operations can qualify as coercive.

Nevertheless, it might be possible to agree on certain non-exhaustive factors that likely would influence the characterization of a foreign information operation during an election as coercive or not. An operation's scale and effects would seem to be highly relevant. There is precedent for looking to these factors in interpreting ill-defined thresholds. For example, the ICJ has pointed to scale and effects when assessing whether a use of force rises to the level of an "armed attack", and states (e.g., Australia) are increasingly using the approach with regard to the threshold for a cyber use of force. Scale and effects would consider factors such as how widespread the impact of the election interference is, how serious its effect on the election is, and perhaps even the nature and significance of the election in question (e.g., municipal versus national).

Another factor that might bear on the determination of whether an information campaign is coercive is the veracity of the information in question. At first glance, it would seem difficult to make the case that the release of truthful information can ever be coercive. After all, at least in theory, the better informed the electorate, the more it is able to participate meaningfully in the election.

But consider the scenario offered above where a foreign state

dominates the information space. Or recall the 2016 Russian meddling, in which genuine but purloined material was released at a point in the election that did not afford the Clinton campaign an opportunity to effectively rebut and recover, thereby skewing voting. In that case, complicating matters was the fact that the truthful information was packaged in a layer of deception regarding the identity of those who acquired it and their affiliation with the Russian state. Had American voters known that the information, even if truthful, was being disseminated by Russia as part of an influence campaign, that knowledge might have caused them to evaluate it differently. Perhaps there should be a presumption that the dissemination of information that is both truthful and complete does not violate international law, but that presumption should be rebuttable in extreme cases.

It would seem easier to describe disinformation campaigns as coercive. The range of possible scenarios is limited only by one's imagination. For instance, artificial intelligence could be used to create fake user profiles (profile pics, names, etc.) in huge numbers to create negative "buzz" about a candidate on social media. Or consider a deep fake in which a candidate purportedly admits to egregious criminal behavior. It is released just before election day when there is no time to counteract its effect, thereby altering the election result. Similarly, take the case of a cyber operation involving a fake website purporting to be that of an influential media outlet that puts out a story as the polls open claiming the candidate has admitted to the criminal activity. The story goes viral and the candidate loses.

Many other factors could come into play in determining whether to style a foreign information (including disinformation) campaign during an election as coercive. For instance, an operation designed to achieve a specific result, such as the election of a particular candidate favored by the foreign state, is probably more likely to be characterized as coercive than one intended merely to cause general electoral disruption in the target state, for instance by using social media to disseminate

disinformation about all the key candidates. Similarly, an operation that exploits specific vulnerabilities in the target state, such as ethnic or religious divisions, presumably would be more likely to be seen to be coercive than one that is simply negative.

C. Obligation to Respect Sovereignty

Foreign activities in cyberspace might also violate the rule of sovereignty. Before discussing how, it must be cautioned that one state, the United Kingdom, has rejected the proposition that cyber activities can amount to a violation of sovereignty, relying instead on the rule of intervention to serve as the bulwark against foreign election interference. However, that stance, which has been discussed in depth elsewhere (see, e.g., here and here), has not been adopted by any other state. On the contrary, a growing number of states, including France, the Netherlands, Germany, Iran, the Czech Republic, Austria, and Switzerland, have taken the opposite position, and, seemingly, so has NATO (with the UK reserving). The analysis that follows proceeds on the basis that the requirement to respect the sovereignty of other states is a primary rule of international law (see Tallinn Manual 2.0, Rules 1-5).

Max Huber famously set forth the classic definition of sovereignty in the 1928 Island of Palmas arbitration: "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State." This formulation contains within it both instances of how sovereignty can be violated.

First, sovereignty can be violated based on an infringement of territorial integrity and inviolability. There is general agreement that a cyber operation causing physical damage or injury in another state qualifies as a violation of its sovereignty. Consensus also appears to have coalesced around treating a relatively permanent loss of functionality of cyber infrastructure as the requisite damage (see, e.g., Czech Republic,

France). While physical damage is unlikely in the election interference context, the US government has warned that foreign governments may try to compromise election infrastructure (functionality) in the upcoming elections.

Unfortunately, there is no such consensus as to a loss of functionality that is temporary or that causes the affected cyberinfrastructure to operate in a manner other than intended, as in making it operate slowly or generate spurious results. This is problematic because such consequences can be expected of election-related hostile cyber operations, a real-world example being the denial of service attacks targeting Ukraine in 2014.

France has addressed hostile cyber operations generating consequences of this nature in its legal doctrine. In 2018, the Ministry of the Armies noted that it would treat "[a]ny cyberattack against French digital systems or any effects produced on French territory by digital means" that is attributable to a state as a breach of its sovereignty. While the precise parameters of the standard are indistinct, France presumably would treat a cyber operation targeting its government election hardware or software or that causes "effects" on other systems, such as a denial of service operation directed at a campaign's website, as a breach of its sovereignty. It remains to be seen whether other states will be willing to go as far in interpreting the territorial aspect of the sovereignty rule.

Second, sovereignty may be violated by cyber activities that interfere with, or usurp, an "inherently governmental function" of the target state. The issue in the election context is interference. An inherently governmental function is one that only states may perform or authorize non-state entities to carry out; conducting elections clearly qualifies. Importantly, there is no requirement that the interference rises to the level of coercion, as is the case with the prohibition of intervention – any interference with the state's ability to perform the function qualifies.

And unlike the violation of sovereignty on the basis of territoriality, there is no requirement of any particular physical or functional effects. The only essential consequence is interference itself.

It is not altogether clear whether all interference with an election is encompassed in the rule. Of course, a foreign state's cyber activity that directly diminishes the government's ability to conduct the election violates that state's sovereignty on this basis. Examples include temporarily disrupting the proper functioning of election hardware and software, blocking access to online government information about the election, and altering that information.

It is somewhat unsettled as to whether cyber activities that are not directed against the government's systems can violate sovereignty. It would seem reasonable that those that indirectly disrupt the smooth execution of the election, such as voter suppression activities, would qualify. As an example, posting incorrect information as to how, where, or when to vote could fairly be characterized as interfering with the state's ability to conduct the election.

The open question is whether cyber activities that involve information or disinformation that does not affect the manner in which the election is carried out ever violate sovereignty. Consider, for instance, operations designed to foster societal division, as in exploiting racial fault lines by means of "dog whistles." If such operations are causally related to the requisite consequences (e.g., by inciting riots that cause damage or injury), a violation of the rule might possibly be made out, but even this remains uncertain.

D. Obligations to Respect Human Rights

There is widespread consensus that human rights must be respected and protected online as they are offline (see, e.g., 2015 GGE Report; 2012, 2014, 2016, 2018 Human Rights Council; Tallinn Manual 2.0, Rules 34-38). Several specific rights loom large in the online election interference context – the freedom of expression; the right to privacy; the right of citizens to participate in public affairs, vote and stand for elections; and the right of all peoples to self-determination. However, the applicability of human rights to cyber election interference operations may be questioned on grounds of extraterritoriality, a much-contested issue in various other contexts. Each of these points will be addressed in turn.

Freedom of expression is guaranteed by both treaty and customary international law. It is enshrined in such instruments as the International Covenant for Civil and Political Rights (art. 19), the Universal Declaration of Human Rights (art. 19) and regional treaties like the European Convention on Human Rights (art. 10). As described in Article 19(2) of the ICCPR, it encompasses the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."

States that interfere with elections abroad implicate the freedom of expression when they, for instance, interfere with candidates' online campaigns (impart) or alter or erase online information about candidates that voters wish to access (seek). As to states countering foreign online election interference, any activity that impedes online expression, such as requiring internet service providers or social media companies to filter, delete, or label data posted or transmitted by the interfering state, must itself be justifiable pursuant to the human rights standards described below.

Like the right to freedom of expression, the right to privacy is a customary right that also finds expression in treaty law (e.g., ICCPR, art. 17; UDHR, art. 12; ECHR, art. 8). It too can be implicated by election interference, as was well illustrated by the exfiltration and public dissemination of private email during the 2016 US presidential elections.

Both treaties and customary law also guarantee the right of all citizens to participate in public affairs, to vote in elections and to stand for election (e.g., ICCPR, art. 25; UDHR, art. 21; ECHR Protocol 1, art. 3; American Convention on Human Rights, art. 23). While international case law has historically focused on internal interference with these rights, there is no reason in principle to exclude interference by third states from their scope (on the extraterritoriality point, see below). Thus, for example, cyber operations resulting in voter suppression would directly impede enjoyment of the right to vote. As for influence operations, the Human Rights Committee has noted (General Comment No. 25, para. 19) that "[v]oters should be able to form opinions independently, free of violence or threat of violence, compulsion, inducement or manipulative interference of any kind (emphasis added)."

None of the aforementioned individual rights are absolute. States may limit their exercise or enjoyment by measures that pursue a legitimate aim, are necessary to achieve that aim, are prescribed by law, and are proportionate (see, e.g., General Comment No. 34, para. 22). However, it is extremely unlikely that electoral interference by a foreign state could satisfy these requirements, if only because it would not be pursuing an aim regarded as legitimate under human rights law.

It has been suggested that the human right to self-determination, which again is protected both by customary and treaty law (ICCPR, art 1; International Covenant on Economic, Social and Cultural Rights, art. 1; UN Charter, arts. 1 and 55), might be implicated by foreign election

interference. Self-determination includes the right of a people to determine their own political arrangements. Those taking the position that the issue of self-determination surfaces in the context of foreign election interference do so on the basis that elections represent the sovereign will of a people with respect to the nature of their governing political system and, therefore, disrupting them interferes with their exercise of self-determination.

The argument is facially plausible, but this interpretation of the right presents numerous challenges. It is a collective, not individual, right, which raises issues as to its enforcement; the right typically applies in the context of the emergence of a state; there are practical difficulties in determining that the interference actually blocked the will of the people; and it is unclear whether the concept of a "people" in international law, which is already unsettled, can refer to the entire population of an established state or only to a sub-group. Nevertheless, this is an interesting proposition that could gain traction in the face of chronic foreign election interference by cyber means, especially when such interference is systematic and large-scale.

Whether any of these human rights apply to foreign cyber election interference depends on the contentious issue of extraterritoriality, that is, whether states owe human rights obligations to those in the territory of another state. After all, election interference operations by a foreign state are extraterritorial by definition. Of course, in the case of specific treaty obligations the answer is to be found through interpretation of the instrument's jurisdictional provisions. The discussion that follows takes on the issue in a general sense.

Restrictive views on the matter hold that human rights do not apply extraterritorially. The United States, for example, has long taken this position with respect to the ICCPR (but see a 2010 US State Department Legal Adviser memorandum). The European Court of Human Rights adopted a somewhat less restrictive (but still restrictive)

position regarding the European Convention on Human Rights in the Bankovic case, which involved the right to life. By the restrictive approaches, even if election interference by cyber means theoretically implicates human rights such as the freedom of expression or the right to privacy, it would not be unlawful because the relevant treaties would not apply in the first place.

The various opposing views argue that extraterritorial cyber operations are covered by human rights law. Under one, the negative obligation to respect human rights (i.e., to refrain from conduct) simply should be understood to apply extraterritorially. By a second, termed the "functional approach," control over the exercise or enjoyment of rights provides a basis for their application (for a discussion of both views, see here). For instance, with respect to the right to life, the Human Rights Committee has interpreted state jurisdiction under the ICCPR as reaching "all persons over whose enjoyment of the right to life [the state] exercises power or effective control. This includes persons located outside any territory effectively controlled by the State, whose right to life is nonetheless impacted by its military or other activities in a direct and reasonably foreseeable manner."

The same logic could be applied to rights such as the freedom of expression or privacy that are implicated by foreign election interference, as they may be impacted as described above by the remotely conducted election interference. Indeed, three distinguished officials have recently asserted that "[t]he right to freedom of expression, which includes the right to seek, receive and impart information and ideas of all kinds, regardless of frontiers, through any media, applies to everyone, everywhere." In this regard, as the Human Rights Committee has noted, it would seem "unconscionable" to interpret human rights law to permit a state to violate human rights on the territory of another state in a way that it "could not perpetrate on its own territory" (see also the German Federal Constitutional Court's judgment on the extraterritoriality of the Basic Law, in which the Court

held that fundamental rights protections apply to surveillance operations abroad, thereby making any subsequent legal policy not to extend protections to other types of transnational cyber operations difficult to reconcile with the judgment).

II. Positive Obligations Implicated by Election Interference

A. Obligation of Due Diligence

This brings us to positive obligations that states have with regard to election interference activities. The ICJ acknowledged a so-called "due diligence" obligation of states to control activities occurring on their territories in its first case, Corfu Channel. In that 1949 judgment, the Court observed that a state has a duty to not "allow knowingly its territory to be used for acts contrary to the rights of other states." The Tallinn Manual 2.0 experts concluded that there was no reason to exclude the rule's application in the cyber context (Rules 6-7); a number of states have come to the same conclusion (see, e.g., Brazil, Estonia, Finland, France, Korea, Netherlands, but see Argentina). However, unable to achieve unanimity on its status as a binding rule of international law in the cyber context, the UN GGE adopted it in its 2013 and 2015 reports as (at the least) a voluntary non-binding norm of responsible state behavior in cyberspace.

Accordingly, whether a state must, as a matter of international law, take action to stop election interference by third states or non-state actors that is being conducted from, or by otherwise using (as in the case of hosting leaked data on a server in a third state or taking remote control of cyber infrastructure from which to mount hostile operations), its territory remains unsettled. Even if so, the Tallinn Manual 2.0 experts cautioned that the due diligence obligation is quite limited in reach. Although the rule applies to hostile cyber operations by both state and non-state actors, the obligation only attaches when the operations are ongoing or imminent (in the sense of a material step having been

taken). Additionally, they must affect an international legal right of the affected state, as well as cause "serious adverse consequences," and the territorial state has to know of the operations in question. In these circumstances, the territorial state will still only be in breach of the obligation if it was feasible to put an end to the operations and it did not do so. Importantly, there is no obligation to look to other states, including the victim state, for assistance, although the territorial state is free to do so.

These limitations loom large in an election interference scenario. Most significantly, the remotely conducted election interference would have to implicate a right of the victim state. The myriad fault lines outlined above in the relevant primary rules would directly affect whether the obligation applies. For instance, a state claiming a due diligence breach on the basis that the election interference implicates the rule of non-intervention would face the uncertainty surrounding the threshold for coercion.

However, there is one significant benefit to the rule of due diligence in the election interference context. In a situation in which a state cannot adequately attribute remote election interference in fact or law to the state from whose territory it is being conducted, it may nevertheless be able to claim a breach of due diligence on the part of that state. The failure of the territorial state to put an end to the election interference then would open the door to countermeasures (see below) that could take the form of cyber operations directed against the source of the interference (see explanation here).

B. Obligations to Protect Human Rights

In addition to the duty to respect human rights, states shoulder an obligation to protect (secure, ensure) the human rights of individuals on their territory, a principle captured in ICCPR (art. 2(1)), and other human rights instruments such as the ECHR. As explained by the Human Rights Committee, "the positive obligations on States Parties

to ensure Covenant rights will only be fully discharged if individuals are protected by the State, not just against violations of Covenant rights by its agents, but also against acts committed by private persons or entities that would impair the enjoyment of Covenant rights." Thus, if harmful cyber interference by another state or a non-state actor is likely to impede, or is impeding, the exercise of protected rights related to the election, the state in which the election is taking place must take those measures at its disposal to prevent or end the interference.

It must be emphasized that unlike the due diligence obligation under general international law, which only applies to ongoing or imminent activities, the human rights obligation to protect requires a state to take reasonable preventive measures in anticipation of remotely conducted election interference that would place protected rights at risk. Moreover, the protective obligation undoubtedly applies because the inability to exercise or enjoy the right in question occurs on the territory of the state conducting the election. It is unclear, however, whether such a protective obligation would extend to individuals located outside the state's territory, such that state A would have a human rights duty to protect elections in state B if A's territory was being used to mount cyber operations against B.

Like due diligence, the obligation is a duty of conduct, not of result. States need only take those actions that are within their capabilities in the attendant circumstances. Factors bearing on feasibility range from cost to technical wherewithal.

III. Response Options

States facing remotely conducted foreign cyber election interference have a number of response options at their disposal. Internally, they may take a variety of measures under their domestic law to protect the integrity of their elections. Such measures, which may, for example, involve the regulation of social media platforms and restrictions on speech that

contains electoral disinformation, have to comply with the requirements of international human rights law cited above. These are regulatory questions of great complexity that will not be addressed here further.

Internationally, states may bring the matter before various dispute resolution fora, such as the ICJ or the European Court of Human Rights, or they may do so before political bodies like the UN Security Council. The Council could even authorize measures under Chapter VII of UN Charter to terminate the operations should it find the election interference to constitute a "threat to the peace." However, a number of self-help measures are also available under international law to victim states.

The option elected by the United States when targeted by Russian election of interference in 2016 was retorsion. Retorsion is an act that, albeit unfriendly, does not violate international law. For instance, the Obama administration imposed sanctions, expelled "diplomatic" personnel and closed Russian facilities in response to Russia's election meddling. Because retorsion involves acts that are not prohibited by international law, a state may engage in it without having to establish that the underlying activities are violating its international legal rights. This may be why the Obama administration elected that course of action.

If the remotely conducted election interference violates international law, the "injured state" may also take countermeasures (ASR, art. 22, Tallinn Manual, Rules 20-25). The difference between retorsion and a countermeasure is that the latter is an act (action or omission) that would be unlawful but for the fact that it is undertaken to compel the offending state ("responsible state") to desist and/or to secure any reparations that might be due for injury suffered (ASR, art. 49). For reasons such as the risk of escalation, some nervousness surrounds the political endorsement of the applicability of countermeasures in the cyber context. Nevertheless, many states have explicitly confirmed their availability in response to unlawful cyber operations (see, e.g., Australia, Estonia, France, Netherlands, United Kingdom, United States).

In this regard, countermeasures are typically thought of as a "hack backs." For instance, the injured state could conduct cyber operations to disable the cyber infrastructure being used by the responsible state to conduct the election interference, an act that otherwise might amount to a breach of the responsible state's sovereignty. However, countermeasures may also be directed at cyber infrastructure other than that involved in the hostile operation; indeed, the countermeasure need not even be cyber in nature so long as it is designed to put an end to the unlawful cyber activity affecting the election or to secure reparations based on that interference.

It should be emphasized that countermeasures are subject to a number of conditions and limitations, such as a requirement of proportionality. Perhaps most significantly, they are only available in response to election interference that violates international law (or a failure to exercise due diligence); if either the element of attribution or breach is missing, the response cannot qualify as a countermeasure and the action remains unlawful.

Finally, a state that is facing a "grave and imminent peril" to one of its "essential interests," irrespective of the source and regardless of whether the peril is the result of an international law violation, may take otherwise unlawful action to put an end to the threat so long as the measures it takes are the only means of doing so and the action does not affect the essential interests of any other state (ASR, art. 25) This so-called "plea of necessity" is a measure limited to exceptional circumstances (Tallinn Manual 2.0, Rule 26).

The conduct of elections is clearly an essential interest in a democracy. Therefore, the determinative question with respect to a particular instance of election interference will usually be whether the consequences are serious enough to merit characterization as "grave." Unfortunately, international law provides no bright line threshold of requisite gravity. But if the peril is grave, an otherwise unlawful action in response to the election interference is permissible.

IV. Concluding Thoughts

It's complicated, to say the least. There are some foreign election-related activities that are clearly unlawful, as when organs of a state conduct cyber operations that affect the ability of the target state to execute the election. Yet, beyond the few unequivocally wrongful cases, multiple fault lines in the international law governing cyber activities will hinder definitive characterization of a particular act of election interference as unlawful. These range from questions of fact and evidence to the unsettled issues surrounding the existence and interpretation of the primary rules. Such issues bleed over into the availability of response options. It is clear that this fog of law demands continued action by states to clarify the rules (see Hollis Report), for until that occurs, states will struggle to determine how to characterize election interference and respond effectively to it.

Acknowledgement: a revised and expanded version of the paper was published at [2021] EHRLR 68.

Protecting Political Discourse from Online Manipulation: the International Human Rights Law Framework

*Kate Jones**

* Associate Fellow, Chatham House; Faculty of Law, University of Oxford.

1 Introduction

Online manipulation of political debate presents a large and expanding threat to democracy. Since first hitting the headlines in the aftermath of the US presidential election in 2016, it is increasingly a hazard of election campaigns and political debate all over the world. Its techniques are being adopted both by overseas, often state-sponsored actors and by domestic political campaigners. Fact-checking, media literacy, and support for robust independent media, while all important, are insufficient defences against covert, developing technologies of manipulation.

Online manipulation campaigns interfere with individual human rights. State manipulation, foreign or domestic, may breach international human rights law. States' human rights obligations require them to take action against manipulation of democratic debate in their own countries, and social media and online search platforms' human rights responsibilities entail that they should tackle manipulation on their platforms by reference to human rights law.

This paper first briefly outlines online manipulation in political debate and campaigning. It then provides an overview of the structure and application of international human rights law to online manipulation. Third, it summarises the content and relevance of key human rights. It concludes by stressing the role of international human rights law in tackling online manipulation.

2 Online manipulation of political debate

Online manipulation of political debate, including election campaigns and referenda, may be conducted by international actors, often orchestrated with state support ("foreign interference operations") or by domestic actors, whether government agency, political party, private actor or individual ("domestic online manipulation campaigns"). Both types of operation rely on online manipulation: deliberate, non-transparent attempts to influence audience reactions and opinions through emotive, shocking, divisive or controversial material whose reach and impact may be deliberately exaggerated and repeated, harnessing tools of amplification in social media or web search optimization. The creation, distribution and audience targeting of online content allows for myriad forms of manipulation, many of them not easily visible to researchers. The boundaries of manipulation have not yet been defined, such that the distinction between legitimate campaigning and manipulation is currently blurry.

Disinformation is one egregious example of manipulation: the intentional sharing of false, distorted or manipulated information in order to cause harm. Its most significant characteristic is not the falsity of the information but the intention to cause harm (true information taken out of context or subjective opinion shared with similar intent can be equally problematic). One prominent monitor of disinformation defines it as comprising "adversarial narratives", narratives often developed from seeds of truth that are manipulated with the aim of creating opposition between societal groups. Disinformation should be distinguished from misinformation, information that is false but is not created or shared with the intention of causing harm.

Another patent example of manipulation is the use of networks of inauthentic accounts to increase the reach of material. Such online manipulation services are openly available online and can easily be purchased. To give a crude example, the more "likes" and comments a

post has (for example, because a political party has bought them or a foreign actor has bots and employees to post them), the more social media algorithms will promote it to the heart of newsfeeds and online debate. Other forms of manipulation are manifold, ranging from those linked to content (for example content that is deliberately divisive of society or undermines trust in its institutions, such as the deliberate sowing of conspiracy theories, rumours, confusion or social discord, discrediting of institutions or prominent individuals) to those linked to distribution (opaque use of advertisements, groups, techniques to distort platform algorithms); to those linked to influence (micro-targeting, co-option of apparently apolitical topics and groups to spread political messages); to use of synthetic techniques (such as deepfakes). Facebook's reporting on "coordinated inauthentic behaviour", Twitter's on "platform manipulation" and Google's on "coordinated influence operation campaigns" each track some of the online manipulation visible to them. The types and scale of manipulation are likely to develop further with emerging data analytics and sentiment analysis technology.

Manipulation is widespread and growing. In 2019 – prior to 2020's COVID-19 "infodemic" – foreign interference operations in political discourse were found to originate from seven countries. The Oxford Internet Institute assessed that domestic organised online manipulation campaigns, run by political parties or government agencies, took place in 70 countries (as compared to 48 in 2018); and that in 26 countries, authoritarian regimes were using computational propaganda to stymie political debate. Inauthentic behaviour was recently assessed to account for over 25% of Twitter traffic between 2 and 20 May 2020, including 50% of traffic related to US conspiracy theories.

3 International human rights law: structure of obligations

International human rights law is an atypical body of public international law in that the obligations it creates for a state are not only owed to other states, but simultaneously to individuals both within its jurisdiction,

and to some extent extraterritorially outside its jurisdiction. Since adoption of the UN Guiding Principles on Business and Human Rights in 2011, it has been widely accepted that business enterprises have responsibilities to respect the norms of international human rights law, without jurisdictional limitation.

International human rights law is therefore relevant to regulation of and accountability for foreign interference operations and domestic online manipulation campaigns in three ways. Regarding foreign interference operations conducted or sponsored by State A in respect of an election in State B, international human rights law is relevant in considering:

3.1 State A's obligations to State B and individuals in State B ("international accountability"), to the extent State A has "extraterritorial jurisdiction" in respect of individuals in State B;

3.2 State B's obligations to individuals (and occasionally groups) within its jurisdiction ("domestic regulation and accountability"); and

3.3 the responsibilities of social media and search engine platforms, wherever located, to respect the human rights of individuals in State B ("corporate responsibilities").

Points 3.2 and 3.3 apply equally to domestic online manipulation campaigns. These are considered in turn below.

3.1 Human rights law: state accountability for foreign interference operations

The UN Human Rights Council has repeatedly affirmed that "the same rights that people have offline must also be protected online". The international nature of foreign interference operations would benefit from an international regulatory response, but there is currently little global impetus for new norms. Existing international human rights law may offer some scope for state accountability for foreign

interference operations, but only to the extent that its norms are ones of extraterritorial jurisdiction (ie State A must respect them as regards individuals in State B).

In other contexts, the prevalent view of states, courts, expert bodies and academics is that the state's obligations under international and regional human rights treaties, as well as customary international law, are primarily owed to individuals within its territory. Over the last 20 years, there has been growing acceptance that the state's civil and political rights treaty obligations are owed to an individual outside its territory if the state has physical power or control over the individual, either personally (for example because the state is detaining the individual overseas) or because the individual is in an area subject to the state's effective control (for example Turkey in respect of Northern Cyprus, Russia in respect of Transdniestria). A minority of states, notably the United States, considers that human rights obligations are always territorial, without extraterritorial exception.

> While this is by no means an established position, some expert bodies and courts may be moving towards the view that the state's duty to respect, or not to interfere with, an individual's human rights has no jurisdictional limits. For example, the UN Human Rights Committee considers that the state's jurisdiction in respect of the right to life extends to "all persons over whose enjoyment of the right to life [the state] exercises power or effective control". Arguably in Jaloud v The Netherlands the Grand Chamber of the European Court of Human Rights, in founding jurisdiction on an extended concept of authority and control over the individual, implicitly took a step in this direction. In the field of surveillance, the UN Human Rights Committee has called on the US to take "all necessary measures to ensure that its surveillance activities, both within and outside the United States, conform to its obligations under the Covenant" and the UN Human Rights Council has adopted preambular language emphasising "that unlawful or arbitrary surveillance and/or interception of communications…violate or abuse the right to privacy… including when undertaken extraterritorially…".

Given these divergences of view, and the lack of consideration of foreign interference operations to date by courts and expert bodies, it is not yet established whether foreign interference operations conducted by State A may violate the human rights of individuals in State B. There may be a trend amongst some states and human rights bodies towards the position that states have a duty to respect, or not to interfere with, an individual's human rights wherever that individual is located. This trend would doubtless be contested by other states.

3.2 Human rights law: domestic state regulation and accountability for online manipulation

To the extent manipulation interferes with human rights, states are obliged not to engage in online manipulation campaigns themselves and to protect the human rights of individuals within their jurisdiction from online manipulation by other foreign or domestic actors. These obligations entail both directly protecting individuals from manipulation (for example by deterrence or sanctions, if appropriate) and exercising monitoring and oversight of platforms' efforts to tackle manipulation.

There are jurisdiction and conflict of laws issues at domestic level. The Human Rights Committee has said that states have a duty to ensure that corporate activities within their jurisdiction, but having a "direct and reasonably foreseeable impact on the [rights] of individuals outside their territory" are consistent with human rights standards, but some states, including the United States and the Netherlands, dispute this view. In practice, a social media platform may face conflicting obligations from the state where it is headquartered to censor content on its platform and from a state where it is operating to respect freedom of expression, or vice versa. While a headquarters state may require a platform to respect human rights globally, the reality is that the platform's only options may be to meet the demands of the state where it is operating or to leave that country.

The human rights engaged by online manipulation campaigns are discussed in section 4 below. States should clearly condemn manipulation campaigns that violate human rights. Unless they do so, we risk a race to the bottom as political parties all over the world adopt online manipulation techniques that are not clearly unacceptable, with platforms fighting a rear-guard action to control them.

States should take appropriate measures to protect their populations from online manipulation campaigns that interfere with human rights. They should begin by requiring much more transparency from platforms, so that they have better insight into the issues, and by conducting a multi-stakeholder conversation to distinguish legitimate political debate from manipulation. States should also take proactive measures to defend society against the effects of that manipulation, for example by supporting a robust independent and diverse media, sponsoring fact-checkers and educating the public.

To date some states have largely left platforms to manage online manipulation, save where manipulation coincides with other online harms concerning freedom of speech and privacy rights (such as the EU's Code of Conduct on Countering Illegal Hate Speech Online and Germany's Network Enforcement Act). Other states have responded to manipulation with blunt measures that violate the right to freedom of expression, for example by banning falsehoods (such as Singapore's Protection from Online Falsehoods and Manipulation Act 2019). In general states have not guided platforms as to how they should strike a balance between fostering open and pluralistic speech and avoiding online manipulation. Some states and regions are working on initiatives in this respect, such as the European Commission's forthcoming European Democracy Action Plan and the United Kingdom's Defending Democracy Programme.

States should not leave platforms to ascertain and implement the implications of human rights law in tackling online manipulation without

guidance, for at least four reasons. First, doing so leaves platforms' efforts to meet their human rights responsibilities vulnerable to political controversy, with platforms at risk from political or commercial pressure to yield to political demands. The ongoing 2020 US election campaign is a vivid illustration. Second, doing so relies on an assumption of political neutrality on the part of social media platforms, which (whether or not justified to date) may not be the case in future. Third, doing so assumes that platforms are immutable, but states should not shy away from requiring changes to platform structures and operating practices if necessary to avoid human rights violations. Fourth, as online manipulation raises novel issues of wide-ranging significance, it is the state which has the democratic mandate and guardianship of the public interest required to perform the sensitive balancing of competing rights and interests required by human rights law in its own national or regional context. Although platforms make decisions in individual cases, they should be guided by states on overarching principles. To the extent that state involvement in guiding platforms may lead to risks of state control over speech and information, states should ensure independent input or oversight.

States' human rights law obligations entail that they should provide appropriate accountability not only for those who engage in online manipulation campaigns, but also for social media and online search platforms. Platforms' total or limited immunity in many jurisdictions in respect of content hosted on their platforms has generated a welcome environment of pluralistic expression, but if retained should be compensated for by other measures of accountability, including platform transparency, independent oversight and regular multi-stakeholder dialogue. Such accountability must be carefully calibrated to encourage good platform behaviour but avoid a chilling effect on speech by incentivising content removal. Domestic and regional litigation testing the application of human rights law to online manipulation campaigns would provide further guidance and accountability for states, social media platforms and political campaigners.

3.3 Human rights law: the corporate responsibility to respect: platforms and online manipulation

While international human rights law does not impose obligations directly on private companies, all business enterprises have a non-binding "responsibility to respect" human rights, endorsed by the UN Human Rights Council as part of the UN Guiding Principles on Business and Human Rights in 2011. This responsibility concerns all the rights in the International Bill of Rights, regardless of where the activity takes place or where those affected are located. It entails that businesses should adopt a clear policy commitment to human rights; a human rights due diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights; and remediation processes in respect of any adverse human rights impacts. It applies in respect not only of the enterprise's own activities, but also in respect of "human rights impacts that are directly linked to [its] operations, products or services by [its] business relationships". Companies should report to external stakeholders on how they address their human rights impacts.

The responsibility of social media platforms to respect human rights has been urged by UN and regional Special Rapporteurs, recognised by the Committee of Ministers of the Council of Europe and, as regards the processing of personal data, by the UN Human Rights Council. Some social media platforms have assumed voluntary commitments in respect of freedom of expression and privacy through membership of the Global Network Initiative. A growing number of platforms have decided to structure their developing content moderation and privacy practices around human rights norms, albeit that their implementation of human rights responsibilities lacks transparency and is nascent, patchy and underdeveloped. Even as regards those platforms which profess commitment to human rights, evidence from the non-Western world, such as Nyabola's on digital democracy in Kenyan politics, is that there is little implementation and that online manipulation is costing fragile political systems dearly. This account was recently borne out by

Facebook whistleblower Sophie Zhang.

To enable guidance from and accountability to states, as well as academic, civil society and media review, platforms should be much more transparent about the manipulation they see, how their operating systems interact with it and the action they take and are planning to develop to counter it, building on the periodic reporting some are already providing.

Leaving aside content moderation and privacy, social media platforms have not expressly structured their efforts to curb manipulation around human rights, particularly freedom of thought and opinion and the right of political participation. Doing so would assist them in structuring their efforts against online manipulation campaigns and in reconciling their responses to manipulation with continued commitment to freedom of expression. The human rights engaged by online manipulation are discussed in section 4 below.

4 The human rights engaged by online manipulation campaigns

This section briefly discusses how online manipulation campaigns may interfere with human rights. It covers the right to participate in public affairs and to vote; the rights to freedom of thought and freedom of opinion; the right to privacy; the right to freedom of expression; and (of arguable relevance) the collective right of self-determination. For the purposes of this section, the rights in the International Covenant on Civil and Political Rights (ICCPR) are discussed and are assumed to reflect customary international law, except where otherwise indicated. Variations between ICCPR and regional human rights treaties are not discussed.

4.1 Right to participate in public affairs and to vote

By Article 25 ICCPR, every citizen is to have the "right and the opportunity…to vote and to be elected at genuine periodic elections…

held by secret ballot, guaranteeing the free expression of the will of the electors". This right includes the right not only to vote, but to engage in public debate and assembly. Foreign interference operations and domestic online manipulation campaigns that impact citizens' ability to engage in democratic debate and voters' ability to glean information and make up their mind freely are incompatible with the right to vote. These may include: interruptions to internet access, such that citizens are unable to access information or participate in debate; interferences with election infrastructure so that voters are unable to exercise their right to vote or to have their vote counted; deliberately misleading voters over how to vote, for example as to the date of the election or where or how they may vote; deliberately distorting voters' ability to form their will freely (see discussion of rights to freedom of thought and opinion, below); and deliberately deterring voters from voting. Deliberate dissuasion of candidates from standing or speaking their views, for example through trolling or incitement to hatred, also interferes with the right.

4.2 Rights to freedom of thought and freedom of opinion

The rights to freedom of thought and freedom of opinion in Articles 18 and 19 ICCPR as well as regional human rights treaties are absolute rights, as the Human Rights Committee has stressed in its General Comments on both articles. They are rights that have traditionally been largely taken for granted, and there is little expert comment or jurisprudence on them. They should now be placed at the centre of discussion of online manipulation, because, as former Google strategist James Williams has described, manipulative techniques can affect individual thoughts and opinions on a scale never seen in the analogue world. Indeed, defining the parameters of freedom of thought and opinion is important not only to curb online interference in political discourse, but also to determine the limits of acceptable techniques of surveillance capitalism.

As Alegre has explained, the rights to freedom of thought and opinion include the right not to reveal one's thoughts or opinions; the right not to have one's thoughts and opinions manipulated, as discussed below; and the right not to be penalised for one's thoughts and opinions.

Individuals of course are constantly receiving influences over their thoughts and opinions, including deliberate attempts to persuade through advertising and political argument. But the digital world amplifies exponentially the opportunities for states and business enterprises to know the thoughts of individuals, to shape them without individuals being aware that this is happening, and for individuals to be penalised or discriminated against on the basis of their views. Both foreign interference operations and domestic online manipulation campaigns aim to manipulate the thoughts and opinions of their target audiences.

The dividing line between acceptable persuasion and unacceptable manipulation is ripe for clarification. In 2005, Nowak suggested that infringements of freedom of thought may be limited to involuntary influence over opinions. Assessing the right to freedom of opinion in detail, Aswad proposes that "deliberate efforts to influence through non-consensual means violate this right when they rise to the level of either overwhelming mental autonomy or manipulating one's reasoning". An interdisciplinary discussion is needed to establish what elements may constitute manipulation that is incompatible with freedom of thought and opinion. Regarding online manipulation campaigns, example elements for discussion might include: an intention to manipulate on the part of the influencer; the influencer's identity, intention and/or methodology being disguised; highly personalised messaging; creation of a false impression that content is authentic; artificial amplification of content.

A multi-stakeholder conversation is needed to establish and advertise these parameters of these rights with the aim of distinguishing domestic online manipulation campaigns from legitimate political campaigning online. As Facebook commented in July 2020, "it's critical that we, as

a society, have a broader discussion about what is acceptable political advocacy and take steps to deter people from crossing the line." To inform that conversation, states, researchers, the media and civil society need much more transparency from social media platforms, commercial purveyors of political influence and political campaigners regarding influence techniques being developed and deployed.

To be clear, restricting manipulative techniques does not restrict freedom of expression: the restriction is not over what is said but over how it is amplified. Restricting manipulative techniques is akin to banning subliminal advertising or hypnosis, which some states have done in the analogue world. Further, not all violations of freedom of thought are violations of the right to privacy. For example, election billboard advertisements have been designed with hidden cameras that detect and report back on the emotional reaction of anonymous viewers, allowing the campaigners to tweak the advertisements so as to maximise positive reactions.

4.3 Right to privacy

The UN Office of the High Commissioner's report on the right to privacy in the digital age found that the right to privacy in Article 17 ICCPR includes a right for the individual to choose not to divulge their personal data, a right to opt out of trading in and profiling on the basis of their personal data, and a right to have their data processed only with their consent or for a legitimate purpose, and with their knowledge. These rights were carefully protected in the analogue era, with individuals required to tick boxes for consent to data retention and sharing. In the digital era, these protections have been swept aside, as online behaviour is widely monitored (often through notional "consent to cookies") and combined with offline profiles to create profiles of voters. European and British data protection laws are inadequate to stem this tide, as their bases for processing ("consent", "democratic engagement", "legitimate interests") are interpreted so broadly as not

to impose meaningful limits. Like political campaigners, those running online manipulation campaigns may be able to gather and use an extensive compilation of personal data without legitimate basis in order to micro-target messages without recipient awareness, consent or choice, inconsistently with the right to privacy.

4.4 Right to freedom of expression

In the battle against manipulation, the right to freedom of expression, which includes the right "to seek, receive and impart information and ideas through any media and regardless of frontiers" (Article 19(2) ICCPR), is a vital bulwark of an open and uncensored internet. Both deliberate interruption of internet connectivity and censorship of communication are clear breaches of this right.

Freedom of expression is further relevant to suppression of manipulation in two ways. First, it constrains responses to manipulation. Such responses must not usually encourage or require platforms to take down disinformation or other manipulative material on the basis of its content (for example, on the basis that it's false); but only to remove, restrict or label it on the basis that it forms part of an online manipulation campaign. Material can exceptionally be removed because of its content if to do so would be lawful, meet a legitimate aim and be necessary for one of the purposes in Article 19(3) ICCPR, such as protection of public health or national security, or if it is hate speech that incites discrimination, hostility or violence. Particularly in the political context, any such restriction must be tightly constrained to avoid its application for authoritarian ends. The French Government's 2018 Law Against the Manipulation of Information, which withstood a freedom of expression challenge to the Constitutional Court, may be an example of a content-based restriction that meets the requirements of Article 19(3). During election campaign periods it permits the most egregious disinformation, of a nature that risks disturbance of the peace or compromise to the outcome of an election, to be suppressed on the order of a judge.

Second, Milanovic and Schmitt argue that disinformation systematically disseminated by the state to its own inhabitants may breach the individual's right to seek and receive information (an element of the right to freedom of expression), especially when accompanied by suppression of true information. Bayer et al posit that the state breaches this right if it fails to ensure an information environment in which individuals can access true or widely-sourced information. Both formulations are novel, and both base breach on the state's distortion of the information environment as a whole. It is important to be clear that these propositions do not assert that all disinformation breaches (or undermines) the right to freedom of expression, nor that states are obliged to suppress all falsehoods or assure the veracity of specific items of information.

4.5 Collective right of self-determination

By virtue of the right of self-determination, all peoples "freely determine their political status" (Article 1(1) of both ICCPR and ICESCR, and generally recognised as customary international law). Unlike the other rights discussed in this paper, the right of self-determination is a collective right. It entails a right for a distinct group within a state to secede in exceptional circumstances, and for a group or an entire population to choose their own form of government within a state. While there is no jurisprudence on the point, it is arguable that it entails that the people of a state have the right to conduct their domestic election process free of foreign interference. Such a right would provide a legal basis for condemnation of all foreign interference operations but otherwise would be unlikely to guide states or social media platforms in management of online manipulation campaigns.

5 Conclusion

Much of the world's political debate now takes place online and free of editorial control. The openness and reach of the internet have

brought great benefits for political debate: tremendous increases in the number and diversity of voices, opportunities to participate, and access to information in politics. But they have also brought manipulation campaigns: distortions to electoral and political discussion, both foreign and domestic, that threaten to undermine democracy.

Manipulation campaigns interfere with the right to freedom of thought and opinion, and the right to participate in public affairs and to vote. When they exploit personal data, they interfere with the right to privacy. When they include discriminatory hate speech, they interfere with the right to freedom of expression. Some argue that systematic state distortion of the information environment breaches the right to seek and receive information, an element of freedom of expression, and that foreign manipulation breaches the right of self-determination.

States must not stymie open political debate, for example by shutting down the internet or banning categories of speech (such as untrue speech, or speech critical of the regime). They must clearly condemn manipulation campaigns that violate human rights, and must not engage in them themselves. States have obligations, and social media and online search platforms have responsibilities, to respect international human rights law in tackling both foreign interference operations and domestic online manipulation campaigns. They should structure their responses by reference to these commitments, and should launch a multi-stakeholder conversation to establish and advertise the parameters of acceptable political advocacy.

Online Electoral Disinformation: A Human Rights Law Perspective

Talita Dias and Tsvetelina van Benthem

I. Disinformation campaigns and their impact on democratic processes

The spread of false information has come to plague digital platforms. Disinformation - the deliberate creation and sharing of false and/or manipulated information that is intended to deceive and mislead audiences, either for the purposes of causing harm, or for political, personal or financial gain[1] – has already taken its toll on electoral processes and the Covid-19 response. The spread of disinformation is possible precisely due to the processes that ensure the functioning of a healthy democracy: unimpeded flows of information and wide-ranging protection of free expression. Disinformation campaigns usually involve the creation, engineering and/or dissemination of false, misleading or sensitive information, especially through the use of fake accounts and bots. Whether foreign or domestic, such campaigns skew political discourse, undermine confidence in electoral processes, and interfere, in sometimes imperceptible ways, with individuals' freedom to form or express their own political opinions, as well as to meaningfully participate in elections.

Social media platforms have become a facilitative environment for the spread of disinformation. Some of the techniques used by digital platforms to attract advertisers – e.g. the use of data mining, personal profiling and other algorithms to target advertising and prioritise content likely to attract attention, such as hateful, violent and divisive rhetoric – have been exploited by actors aiming to influence political processes. One example of an institution routinely mounting concerted disinformation campaigns abroad is the Russia-based Internet Research Agency.[2]

1 This is the definition adopted by the UK Digital, Culture, Media and Sport Committee, Disinformation and 'fake news': Interim Report: Government's Response to the Committee's Fifth Report of Session 2017-2019 Fifth Special Report of Session 2017-2019, House of Commons (2018), p. 2.
2 Dawson and Innes, 'How Russia's Internet Research Agency Built its Disinformation Campaign' (2019); Diresta et al (2018), The Tactics and Tropes of the Internet Research Agency.

Disinformation campaigns can be undertaken by a range of actors and can be confined to a domestic setting or contain an extraterritorial element. A number of scenarios can be envisaged: 1. State authorities mounting disinformation campaigns abroad in an attempt to influence foreign elections; 2. State authorities spreading disinformation for the purposes of manipulating the political process in their own State; 3. Non-State actors spreading disinformation in their own State; 4. Non-State actors spreading disinformation regarding political processes in States outside their own. These scenarios implicate different State obligations. Scenario 1 likely engages States' duty not to infringe upon other State's sovereignty, to the extent that the disinformation campaign carried out by a foreign State affects the target State's inherently sovereign functions (the right to conduct elections). There has been some debate as to whether coercion, as an element of the principle of non-intervention, encompasses deception or influence such as is characteristic of disinformation campaigns.[3] However, most scholars and States agree that the bar for coercion must be set at a high threshold, requiring pressure or compulsion on the part of the coercing State.[4] This means that most instances of disinformation would fall outside the scope of non-intervention. All scenarios seem to engage States' general due diligence obligations not to knowingly allow their territory or infrastructure under their control to be used to affect the rights of other States (the Corfu Channel principle) or cause significant adverse consequences thereto (the 'no-harm' principle).

Most importantly for our purposes, the four scenarios also seem to be subject to States' negative (or horizontal) and positive (or vertical) duties to refrain from violating and to protect individual human rights against the acts of other States or non-States actors under treaty and customary international law. This is so to the extent that several human rights, such as the right to vote and to form and express one's opinion,

3 Milanovic and Schmitt, 'Cyber Attacks and Cyber (Mis)information Operations during a Pandemic', Journal of National Security Law & Policy (forthcoming), at 19; Tsagourias, 'Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace' (EJIL: Talk!, 26 August 2019).
4 Moyniham, 'The Application of International Law to State Cyberattacks Sovereignty and Non-intervention', Chatham House Research Paper, December 2019, at 28.

presuppose individual freedom, i.e. the free and unimpeded exercise of the right in question. Crucially, not only coercion but also deception may vitiate one's freedom of action. In the case of human rights treaties, States' obligations are triggered by the existence of 'jurisdiction', which may be defined by territorial, personal and/or functional criteria, as discussed below. This background paper seeks to assess the extent to which mis- and disinformation may be limited under international, regional and domestic human rights law.

II. Jurisdiction in Human Rights Treaties

In the context of human rights treaties, 'jurisdiction' delineates the scope of a State's power and responsibility over individual rights. Indeed, a State can only be required to respect, protect and ensure the human rights over which it has effective control. To this extent, jurisdiction is a triggering condition to many human rights treaty obligations. There is no question that States have sovereign power over their own territory, and so that human rights jurisdiction is primarily territorial. Likewise, if a State exercises effective control over territories or areas beyond its territory, jurisdiction also extends to those geographically defined spaces.

Beyond this spatial conception, jurisdiction may be established on the basis of physical control or authority over individual right-holders.[5] This is what is known as the 'personal' model of extraterritorial jurisdiction and most human rights bodies and commentators agree that it applies to both negative and positive human rights obligations, at least in some circumstances.[6] This is so to the extent that control over individuals may be exercised through the activities of State agents abroad, whether to respect, protect or ensure at least the human rights implicated in the situation.[7]

5 HRC, General comment no. 31 [80], The nature of the general legal obligation imposed on States Parties to the Covenant, CCPR/C/21/Rev.1/Add.13, 26 May 2004, § 10.

6 Milanovic, Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy (2011), at 119. But the ECtHR has been reluctant to recognize this model in relation to extraterritorial kinetic force in the absence of governmental control (see ECtHR, Banković and others v. Belgium and others, Appl. no 52207/99, Decision of 12 December 2001, paras 74-82; and ECtHR, Al-Skeini and others v. United Kingdom, Appl. no 55721/07, Judgment of 7 July 2011, paras 136-137). For a recent analysis, see Milanovic, 'The Murder of Jamal Khashoggi: Immunities, Inviolability and the Human Right to Life', 20 Human Rights Law Review (2020) 1, at 23-24.

7 See e.g. Inter-American Commission on Human Rights (IAComHR), Coard et al. v. United States, Re-

Several human rights bodies have also expressed the view that jurisdiction extends extraterritorially through the activities of entities, such as companies, which are incorporated or located in a State's territory or are otherwise subject to its control. This model focusses on the extraterritorial effects of personal control: jurisdiction covers the activities of the said entities when these have a direct and reasonably foreseeable impact on the human rights of individuals extraterritorially.[8] As such, a State's positive duties concern the rights that may be infringed by said private entities.[9] While endorsed by the Human Rights Committee and the Inter-American Court of Human Rights, this model remains controversial before other human rights bodies.[10]

Lastly, the Human Rights Committee has advanced a more expansive approach to extraterritorial jurisdiction, grounded in the exercise of control over the enjoyment of the rights in question, regardless of any physical control over territory, the perpetrators or the individual victim.[11] While this functional approach to jurisdiction[12] has been accepted in respect of negative human rights duties,[13] many oppose

port N. 109/99, 29 September 1999, para 37; Al-Skeini, supra note 6, paras 136-139.

8 HRC, Human Rights Committee, General comment No. 36 (2018) on article 6 of the International Covenant on Civil and Political Rights, on the right to life, CCPR/C/GC/36, 30 October 2018, § 22, with respect to the right to life; CESCR, General Comment No. 14 (2000), The right to the highest attainable standard of health (article 12 of the International Covenant on Economic, Social and Cultural Rights), E/C.12/2000/4, 11 August 2000, § 39; CESCR, General Comment No. 15: The Right to Water (Arts. 11 and 12 of the Covenant), UN Doc E/C.12/2002/11, 20 January 2003, § 33; CESCR, Statement on the Obligations of States parties regarding the corporate sector and economic social and cultural rights, UN Doc E/C.12/2011/1, 20 May 2011, § 5; IACtHR, Advisory Opinion OC-23/17 of November 15, 2017 Requested by the Republic of Colombia: The Environment and Human Rights, 15 November 2017, paras 101-102. See also Milanovic and Schmitt, supra note 3, at 29-30.

9 See Besson, Due Diligence and Extraterritorial Human Rights Obligations – Mind the Gap!', 9:1 ESIL Reflections (2020) 2, at 2.

10 See Besson, ibid.

11 HRC, General Comment 36, supra note 8, § 63.

12 See Shany, 'Taking Universality Seriously: A Functional Approach to Extraterritoriality in International Human Rights Law', 7 The Law & Ethics of Human Rights (2013) 47.

13 Milanovic, Extraterritorial Application, supra note 6, at 209; Goodman, Heyns and Shany, Human Rights, Deprivation of Life and National Security: Q&A with Christof Heyns and Yuval Shany on General Comment 36 (2019), available at https://www.justsecurity.org/62467/human-life-national-security-qa-christof-heyns-yuval-shany-general-comment-36/, at 1-2; HRC, Sergio Euben Lopez Burgos v Uruguay, Human Rights Committee (HRC) Communication No 52/1979, UN Doc CCPR/C/13/D/52/1979, 29 July 1981, § 12.3; Lilian Celiberti de Casariego v Uruguay, HRC Communication No 56/1979, UN Doc CCPR/C/13/D/56/1979, 29 July 1981, para 10.3; ECtHR, Issa and others v. Turkey,

its applicability to positive human rights obligations, fearing the lack of necessary governmental infrastructure or powers beyond a State's territory or spatial control.[14] However, the practical impact of adopting such jurisdictional model for positive obligations should not be overstated: any due diligence obligation only extends insofar as the duty-bearer has the capacity to adopt the protective or preventive measures in question.[15] Capacity, in this context, includes the ability to influence the behaviour of the perpetrators,[16] the unpredictability of certain events, the availability of resources, the duty to respect and protect other human rights, and other international obligations.[17] Thus, States are not required to do the impossible or to discharge a 'disproportionate burden',[18] but are expected to adopt measures that are available and reasonable in the circumstances.[19] As in any other jurisdictional model, the requirement of 'capacity' to act overlaps with and modulates the notion of extraterritorial jurisdiction over the enjoyment of human rights.[20]

When it comes to online disinformation campaigns taking place on social media or other virtual platforms, such as private messaging applications, the challenge is to establish jurisdiction over 'cyberspace'. Despite the name, 'cyberspace' is not a virtual reality world where no actual harm results from individual or collective action. Quite the contrary: it includes the Internet as well as other information and communications

Appl. no. 31821/96, Judgment of 16 November 2004, para 71.

14 See, e.g., the account of the debate in Milanovic, The Murder of Jamal Khashoggi, supra note 6, at 19-20; and Milanovic, Extraterritorial Application, supra note 6, at 209, 210-212, 219-220.

15 For example, the ICESCR has no express jurisdictional threshold and yet most of its obligations are positive ones, i.e. duties to protect and ensure social, economic and cultural human rights.

16 Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro), Judgment, 26 February 2007, ICJ Reports (2007) 43, para 430.

17 Cf. ECtHR, Osman v. United Kingdom, 87/1997/871/1083, Judgment of 28 October 1998, para 116.

18 Ibid.; see also ECtHR, Nicolae Virgiliu Tănase v. Romania, Appl. no. 41720/13, Judgment of 25 June 2019, para 136.

19 ECtHR, McCann and Others v. United Kingdom, Appl. no. 19009/04, Judgment of 27 September 1995, para 151; IACtHR, Velasquez Rodriguez v. Honduras, Judgment (Merits), 29 July 1988, para 167. See also The Netherlands, Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace — Appendix: International law in cyberspace (2019), at 4; and Republic of Korea, Comments on the pre-draft of the OEWG Report (2020), at 5.

20 Besson, supra note 9, at 5.

technologies or networks which are often spread across national boundaries. These have not only a logical layer, comprising software (information-processing applications) and the data they process, but also a physical and personal lawyer: the former include all hardware on whose substrate software operate (e.g. cables, radio waves, computers and other devices), while the latter covers all individuals who operate or use such technologies, including victims and perpetrators. Thus, while the territorial, spatial and personal models may cover certain forms of online disinformation (to the extent that a State has physical control over the territory, physical infrastructure or the right-holders in question), the functional model of jurisdiction is one which most widely captures the phenomenon.

III. The spread of false information as protected speech

Freedom of expression is protected under customary international law and international instruments, most prominently, the International Covenant on Civil and Political Rights (ICCPR) and the Universal Declaration of Human Rights. The same right is found in regional human rights instruments, such as the African Charter on Human and Peoples' Rights (ACHPR), the American Convention on Human Rights (ACHR) and the European Convention on Human Rights (ECHR).

Under Art. 19(2) of the International Covenant on Civil and Political Rights (ICCPR), '[e]veryone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.' While the scope of free expression is wide, this right is not absolute. It can be limited according to the test provided for in Art. 19(3): restrictions are permitted to the extent that they are provided by law and necessary to respect the rights or reputations of others; or to protect national security, public order *(ordre public)*, public health or morals.[21] Rights that may be affected or undermined by online

21 Art. 19(3) ICCPR.

disinformation, particularly in context of elections, and thus justify limiting freedom of expression include: a) freedom of thought and opinion[22] b) freedom to seek or impart information;[23] c) freedom of expression of targeted audiences;[24] d) privacy;[25] and d) freedom to vote and participate in public affairs.[26]

Likewise, under Art. 20 ICCPR, 'Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.' While the Human Rights Committee, in its General Comment 34,[27] has taken the view that limitations based on Art. 20 should still comply with the test under Art. 19(3), this view has been subject to criticism. In particular, some have suggested that the speech envisioned in Art. 20 does not fall within the protective scope of Art. 19 in the first place.[28]

Addressing the specific context of elections, the 2014 Report by the United Nations (UN) Special Rapporteur on Freedom on Opinion Expression calls upon states to intensify their efforts 'to promote the pluralism of the media and ensure a plural political debate, ensure transparency in the promotion and financing of political campaigns, and guarantee accountability and fair enforcement of political regulations to prevent those in power from taking advantage [...] to dominate and manipulate public debate'.[29] Similarly, in 2017, the then UN Special Rapporteur on Freedom of Opinion and Expression, along with the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of

22 Art. 18 ICCPR.
23 Art. 19 ICCPR.
24 Ibid.
25 Art. 17 ICCPR.
26 Art. 25 ICCPR
27 General Comment 34 (2011), para. 50.
28 OSCE Representative on Freedom of the Media, Propaganda and Freedom of the Media, Non-paper (2015), p. 17
29 UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report of Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Human Rights Council, 26th session, UN Doc A/HRC/26/30 (2 July 2014).

Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, issued a Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda.[30] In that Declaration, while noting that 'the human right to impart information and ideas is not limited to "correct" statements, that the right also protects information and ideas that may shock, offend and disturb, and that prohibitions on disinformation may violate international human rights standards', stressed that 'this does not justify the dissemination of knowingly or recklessly false statements by official or State actors.[31] A thread that runs throughout the Declaration is the careful balance that States need to strike between protecting freedom of expression, including by not imposing blanket bans on 'false news', and protecting the rights of others, including freedom of thought and expression, privacy and free participation in elections.

The 20th anniversary Joint Declaration on Challenges to Freedom of Expression in the Next Decade,[32] adopted in July 2019 by the free speech mandate holders within the UN, OAS, OSCE, and the ACHPR, provides specific guidance on how states can protect freedom of expression whilst tackling disinformation as well as avoiding private censorship. In particular, it urges states to adopt:

> 'Regulatory measures that address the ways in which the advertising-dependent business models of some digital technology companies create an environment which can also be used for viral dissemination of, inter alia, deception, disinformation and hateful expression. […]
> Human rights sensitive solutions to the challenges caused by disinformation, including the growing possibility of "deep fakes", in publicly accountable and targeted ways, using approaches that meet the international law standards of legality, legitimacy of objective, and necessity and proportionality.' [33]

30 The declaration is available here.
31 Ibid, preambular paragraph 7.
32 Available here.
33 Para 3(b) and (e).

IV. Existing international, regional and selected domestic frameworks regulating harmful speech

Although spreading lies or false rumours is in principle be covered by the right to freedom of expression, it can be limited to the extent that it amounts to harmful speech. Under Article 19(3) ICCPR, four conditions must be observed before such right can be limited to contain the spread of disinformation.[34] First, legality, which means that any limitation must be provided by duly enacted laws that are precise, public and transparent, as well as accompanied by procedural safeguards. Second, legitimacy, i.e. any limitation must be adopted to protect the rights or reputations of others or to protect national security, public order, public health or morals. In the case of disinformation, legitimate grounds for limitation may include a) the protection of other individuals' freedom of expression, thought, privacy and their right to freely participate in elections, as explained below; b) the protection of individuals' right to health and the healthcare sector, in case false information risks jeopardizing public health; and c) the protection of free elections, which may be hindered by the spread of false, misleading or sensitive information about electoral processes (e.g. where and how to vote) or candidates. The third condition is necessity, which requires any limitation to be a measure directly related to the interest protected as well as a measure of last resort, meaning that no less restrictive measure was available. Fourthly, proportionality requires a balancing exercise between freedom of expression and the rights or interest protected: the limitation to the former must be calibrated to the protection of the latter, including its relative importance.

These conditions suggest that only the most serious forms of online influence or information operations may be limited or prohibited consistently with international human rights law. As seen earlier, the malicious purpose of the perpetrator, consisting of intentional or reckless manipulation of audiences, seems to be the key marker of

34 See UNGA Res A/74/486, para 6.

disinformation campaigns that ought to be limited or prohibited under international human rights law. In contrast, so-called misinformation, i.e. the unintentional dissemination or sharing of false or misleading information, is less serious given the lack of planning, targeting or engineering of information by the content spreader. Thus, even if misinformation could lead to serious harm, it may be unnecessary and/or disproportionate to combat it with through stringent measures such as automatic content blocking. Instead, it should be tackled by using less restrictive means which are proportionate to their gravity, such as digital and media literacy campaigns, fact-checking and the flagging or tagging of inaccurate content. Cases of misinformation are thus less straightforward and must be resolved through even more careful balancing of the rights implicated.

The Joint Declaration on Freedom of Expression and Elections in the Digital Age,[35] recently adopted on 20 April 2020 by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, and OAS Special Rapporteur on Freedom of Expression, further specifies how such requirements should play out in the context of electoral dis- or misinformation:

> 'States should ensure that any restrictions on freedom of expression that apply during election periods comply with the international law three-part test requirements of legality, legitimacy of aim and necessity, which implies the following:
>
> 1) There should be no prior censorship of the media, including through means such as the administrative blocking of media websites or Internet shutdowns.
>
> 2) Any limits on the right to disseminate electoral statements should conform to international standards, including that public figures should be required to tolerate a higher degree of criticism and scrutiny than ordinary citizens.

35 Available here.

> 3) There should be no general or ambiguous laws on disinformation, such as prohibitions on spreading "falsehoods" or "non-objective information".
>
> 4) Any limits imposed on media reporting on public opinion polls during elections should also be in strict conformity with the three-part test.'[36]

Likewise, according to the 2020 Joint Declaration, when imposing restrictions on freedom of expression during elections:

> 'i. States should consider supporting positive measures to address online disinformation, such as the promotion of independent fact-checking mechanisms and public education campaigns, while avoiding adopting rules criminalising disinformation.
>
> ii. States should adopt appropriately clear and proportionate laws that prohibit the dissemination of statements which are specifically designed to obstruct individuals' right to vote, such as by intentionally spreading incorrect information about where or when to vote.'[37]

Another area of concern in the context of electoral mis- or disinformation is political advertising. In this regard, the 2020 Joint Declaration recommends that states adopt rules for election spending that provide for transparency of political advertising.[38] The Declaration also stipulates that states should preclude 'targeted political advertising, based on personal data [...] especially during election periods, unless those individuals have consented to the use of their personal data for this purpose'.[39] The 2020 Joint Declaration also calls upon states to exempt all media outlets from liability during election periods for disseminating statements made directly by parties or candidates, unless the statements have specifically been held to be unlawful by an independent and impartial court or regulatory body, or constitute incitement to violence.[40]

36 Para 1(a)(iii).
37 Para 1(a). Emphasis added.
38 Para 1(b)(iv).
39 Para 1(b)(vi).
40 Para 1(b)(i).

Mis- or disinformation may also be limited under Article 20 ICCPR to the extent that it amounts to advocacy of hatred on national, racial, religious or other internationally protected grounds that constitutes incitement to discrimination, hostility or violence.[41] Under this provision, states are required to prohibit this type of harmful speech, which must involve not only advocacy of hatred, but also incitement that is likely to result in discrimination, hostility or violence.[42] However, prohibition need not occur through criminalisation, which must be reserved to the most serious cases.[43] In line with the principles of necessity and proportionality, less restrictive measures include public statements by societal leaders that condemn hate speech and foster tolerance and intercommunity respect, education and intercultural dialogue, expanding access to information and ideas that counter hateful messages, and the promotion of and training in human rights principles and standards.[44] These measures tend to be more effective in tackling the root and systemic causes of national, racial or religious hatred and have been recently recommended by the UN Secretary-General in the UN Strategy and Plan of Action on Hate Speech.[45]

Limitations to harmful speech have also been recognised within regional and national human rights systems.

a. Americas

In the context of the American Convention on Human Rights (ACHR),[46] the requirements for limiting freedom of expression are tight, mirroring the ICCPR's standards. Specifically, Article 13 ACHR provides that freedom of expression shall not be subject to prior censorship, and any subsequent imposition of liability shall be expressly established by law to the extent necessary to ensure respect for the rights or reputations of others, or the protection of national

41 UNGA Res A/74/486, para 9.
42 Ibid, para 8
43 Ibid.
44 Ibid, para 18
45 Available here.
46 1114 UNTS 123

security, public order, or public health or morals. However, under the ACHR, speech that constitutes propaganda for war and any advocacy of national, racial, or religious hatred that incites to violence must be criminalised. Many states in the region also provide for strong intermediary liability protection by law.[47] Section 230 of the United States Communications Decency Act[48] generally provides immunity for providers of "interactive computer service[s]" that host or publish information about others. Similarly, the intermediary liability regime in Brazil requires a court order to restrict particular content.[49] At the same time, some countries have adopted legislation to enhance transparency in political advertisement, especially during elections. For instance, Canadian law requires online platforms to keep and maintain a digital registry of all regulated ads related to federal elections, indicating the names of agents who authorised them and any partisan advertising and election advertising that was published on the platform during election periods.[50] Likewise, in Argentina, political ads must be paid by credit card with full disclosure of the purchaser's identity and the registration of political parties' social media accounts.[51] In the United States (US), following reports of Russian election meddling in 2016, the Honest Ads Act Bill was introduced by Congress. The Act would require online platforms to keep copies of ads, make them public and keep tabs on who is paying and how much. The Bill is currently under discussion before the US Senate.[52]

47 A/HRC/38/35, para 15.
48 47 U.S.C. § 230
49 Arts. 18-19, Marco Civil da Internet (Brazilian Civil Rights Framework for the Internet), L12965.
50 US Congress Library, Government Responses to Disinformation on Social Media Platforms: Comparative Summary, available at https://www.loc.gov/law/help/social-media-disinformation/compsum.php.
51 Ibid.
52 S.1356 — 116th Congress (2019-2020).

b. Europe

In the European context, although the European Court of Human Rights (ECtHR)has stressed that freedom of expression protects the kinds of speech that may offend, shock or disturb,[53] it has been deferential to member states when it comes to limitations to freedom of expression.[54] For example, the Court and its predecessor, the European Commission on Human Rights, have held that legislation criminalising Holocaust or genocide denial, found in several European states such as France, Germany and Austria is consistent with Article 10 of the European Convention on Human Rights.[55] Also in Europe, the 2018 Final report of the High Level Expert Group on Fake News and Online Disinformation,[56] set up by the European Commission, recommends a number of measures to, inter alia, enhance transparency of online news and promote media and information literacy. These are grounded in the principles of accountability, necessity, proportionality, multi-stakeholderism, transparency and clearly defined principles.[57] Among their specific recommendations for addressing online disinformation are: a) multi-stakeholder collaborations to independently identify, monitor, document, and alert citizens to hostile "information operations" from foreign states or domestic groups, especially in advance of elections); b) monitoring of social streams by independent fact-checkers, source verification, and forensic analyses of images and videos at scale and speed; c) demonetisation of false and harmful information for profit; and d) clear identification of sponsored or paid for content, as well as the use of robots.[58] Although European Union (EU) e-commerce directive protects intermediaries from liability,[59] the European Commission has recommended that EU member states

53 Handyside v the United Kingdom, ECtHR, Application No. 5493/72, Judgment, 7 December 1976, para. 49

54 See Council of Europe, "Hate speech", fact sheet, October 2019.

55 M'Bala M'Bala v France, ECtHR, Application no. 25239/13, 20 October 2015; Honsik v Austria, decision of the European Commission of Human Rights, 18 October 1995; Marais v France, decision of the Commission of 24 June 1996;

56 Available here.

57 Ibid, at 20.

58 Ibid, at 22-23

59 Directive No. 2000/31/EC of the European Parliament and of the Council of 8 June 2000.

institute legal obligations for active monitoring and filtering of illegal content.[60] In line with this recommendation, Germany's network enforcement law (NetzDG) requires large social media companies to remove content inconsistent with specified local laws within 24 hours, with penalties of up to €50 millions or non-compliance.[61] Since 2018, France also has put in place stringent rules against the manipulation of information during electoral campaigns and in the three months preceding an election.[62] This law covers the dissemination of inexact allegations or imputations, or news that falsely report facts, with the aim of changing the sincerity of a vote.[63] It gives authorities the power to remove fake content spread via social media and even block the sites that publish it, whilst requiring platforms to publish who has purchased sponsored content or campaign ads and for what price.[64]

In Eastern Europe, some states have in place tight limits on harmful online content and disinformation operations. Russian law, for example, authorises the blockage of information found to constitute fake news, as well as of content that offends human dignity and public morality or shows obvious disrespect for the Russian Federation, its Constitution, or its legal authorities. These are also punishable by fines and administrative detention.[65] 'Fake news' is defined broadly to include 'socially significant' disinformation that, inter alia, might cause mass violations of public order or public security, or interfere with vital state interests such as transportation, social infrastructure, credit institutions, or modes of communication or industry and energy enterprises.[66] The same law also holds social networks accountable for inaccurate comments that users post[67] Websites that have a commenting feature and amass

60 European Commission, recommendation on measures to effectively tackle illegal content online (5 March 2018).
61 Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act), July 2017.
62 Art. 1, LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information.
63 Ibid.
64 Ibid, Art. 10.
65 Davlashyan and Fiorentino, Euronews, 'What is Russia's new 'fake news' law all about?'. See also here.
66 Ibid.
67 Ibid.

more than 100,000 visitors every day are required to remove false comments within 24 hours or be fined up to 50 million rubles.[68] All news broadcasters are also required to disclose the identity of those responsible for disseminating information and network providers may be required to grant full access to their hardware or software by investigative bodies.[69] In Belarus, amendments to the country's media laws allow the government to prosecute people who spread false information online, as well as block social media and other websites if found in violation of the law.[70]

c. Africa

The African Charter of Human and People's Rights[71] also protects freedom of expression in its Article 9. The provision generally provides that every individual shall have the right to receive information and to express and disseminate their opinions within the law, without laying out requirements for limitations to this right. However, earlier this year, the ACHPR has adopted 'Declaration on Principles of Freedom of Expression and Access to Information in Africa',[72] which provides specific guidance on the interpretation and application of this right online. There, the Commission has noted that states parties may only limit the exercise of the right to freedom of expression and the right of access to information, if the limitation is provided by law, pursues a legitimate aim, is necessary and proportionate, as well as compatible with the African Charter and international human rights standards.[73] Similarly, to existing international standards, the Declaration provides that speech that merely lacks civility and respect for the rights of others or which offends or disturbs must not be prohibited or sanctioned.[74] Nevertheless, any speech that advocates for national, racial or religious hatred which constitutes incitement to discrimination, hostility or

68 Ibid.
69 Ibid.
70 TUT News, 'Sometimes forums are dirt: The introduction of criminal liability for false information is discussed' Читать полностью. See also here.
71 CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982).
72 Available here.
73 Ibid, Principle 9.
74 Ibid, Principle 23(3).

violence shall be prohibited by law.[75] Although the Declaration does not contain specific guidance on tackling online disinformation, it refers to states' obligation to develop a regulatory media environments, which are independent from commercial and other types of undue influence.[76] Several African states have put in place laws that criminalise or otherwise prohibit 'fake news'. This is the case, for instance, of Burkina Faso, which in 2019 adopted a law punishing the publication of "fake news" information compromising security operations, false information about rights abuses or destruction of property, or images and audio from a 'terrorist' attack.[77] In Egypt, two laws adopted in 2018 not only punish platforms that publish disinformation but also require them to obtain licenses before they can operate and allows the country's Supreme Media Council to block any harmful content that threatens national security, the national economy, disturbs the public peace, or promotes discrimination, violence, racism, hatred, or intolerance.[78] Likewise, a 2018 Kenyan Law criminalises 17 types of cybercrime, including cyberbullying, espionage and computer forgery and disinformation.[79] Under this law, those who knowingly share false or misleading information in an attempt to make it look real can be fined up to 5,000,000 shillings (nearly US$50,000) or imprisoned for up to two years.[80]

d. Middle East

In the Middle East, the 2004 Revised Arab Charter on Human Rights[81] recognises freedom of expression in terms similar to the ICCPR. Article 32 of the Charter guarantees the right to information and to freedom of opinion and expression, as well as the right to seek, receive and impart information and ideas through any medium, regardless of

75 Ibid, Principle 23(1).
76 Ibid, Principle 12.
77 Sentinel News Service, 'Burkina Faso Orders Stiff Prison Term for "Fake News"', 11 July 2019. See also here.
78 Law No. 175 of 2018 on Anti-Cybercrime and Law 180 of 2018 Regulating the Press and Media. See here and here.
79 The Computer and Cybercrimes Bill, 2017. See also here and here.
80 S 12, The Computer and Cybercrimes Bill, 2017.
81 12 International Human Rights Repository 893 (2005).

geographical boundaries. It also stipulates that those rights 'shall be exercised in conformity with the fundamental values of society and shall be subject only to such limitations as are required to ensure respect for the rights or reputation of others or the protection of national security, public order and public health or morals'. However, there is no specific guidance on the interpretation and implementation of this right at the regional level. When it comes to harmful speech and online disinformation, several Middle Eastern states have adopted stringent laws and other regulatory measures. For example, the United Arab Emirates (UAE) require licensing by its National Media Council for electronic advertisements and for any other electronic activity deemed appropriate by authorities.[82] The UAE also require the blocking or removal of online content that promotes rioting, hatred, racism, sectarianism, or damage to or disturbances of the public order, harm to national unity or national symbols; public morals; or the reputation, prestige, or stature of the state or any of its institutions, its royal family, or high public officials.[83] Disinformation is punishable by imprisonment and a fine in the UAE.[84] In Israel, the Central Election Committee has extended transparency requirements previously applicable by legislation to printed advertisements to advertisements disseminated on the internet.[85] These requirements apply to the disclosure of identifying information of the person, candidate, or candidates' list on behalf of whom the election advertisement was published.[86] Following a 2019 Supreme Court ruling, the Israeli government also banned the publication of anonymous internet advertising on any platform ahead of the 2019 election.[87]

82 National Media Council, Electronic Media Regulation of 2018. See also here.
83 Arts 24, 28 and 29, Federal Law No. 5 of 2012.
84 Ibid.
85 Elections (Modes of Propaganda) Law, 5719-1959, SH 5719 No. 284 p. 138, as amended.
86 Ibid, § 2A2, id. at 53.
87 Election Case 3/21 Shahar Ben Meir v. Naftali Benet, Minister of Education et al., CEC for the 21 Knesset (2019).

d. Asia

In Asia, there are no binding human rights treaties, but only a non-binding human rights declaration adopted by the ASEAN. The declaration nonetheless recognises some of its member states' human rights obligations under customary international law.[88] One of such rights is freedom of opinion and expression.[89] Several Asian countries have specific laws for tackling harmful speech and online disinformation in particular. For instance, China has one of the most comprehensive and strictest legal frameworks to address harmful content and online disinformation, with significant ex ante limitations on freedom of expression.[90] First, it requires social media platforms to be licensed,[91] and their users must register their real names and other identity information with service providers, meaning that internet anonymity is significantly restricted.[92] Chinese network operators must also monitor, report, and remove from their platforms content deemed by authorities to be false and capable of endangering the state economy, social order, and national security.[93] Since 2016, the spread of false information that seriously disturbs public order through an information network or other media constitutes a crime punishable by up to seven years in prison.[94] And in 2017, a new law was introduced that requires social media platforms to exclusively republish and link to news articles from registered news media.[95] Since 2019, China requires microblogging sites to highlight and refute rumours on their platforms.[96] Other Asian states with stringent laws against online disinformation include Malaysia (where online disinformation is a crime since 2018),[97] Singapore (which has criminalised the dissemination or sharing of false

88 ASEAN, 'Human Rights Declaration' (18 November 2012).
89 Ibid, para 23.
90 See here.
91 Art. 2, State Council, Administrative Measures on Internet Information Services (2000).
92 Art. 24, PRC Cybersecurity Law (2017).
93 Ibid, Arts 12 and 47.
94 Ibid, Arts. 70 and 74.
95 Order of the National Internet Information Office, Provisions on the Administration of Internet News Information Services (2017).
96 Administrative Regulations on Microblog Information Services (2019). See also here.
97 Anti-Fake News Act 2018 (Act 803). See also here.

information online since 2019),[98] Thailand (which has expanded the 2007 Computer Crime Act to cover 'fake news'),[99] Vietnam (whose 2019 Cyber Security Law requires platforms to delete content at the government's request and internet service providers to disclose user data so that the government can trace their origin),[100] Cambodia (where the government can block media that threatens national security and the publication of 'fake news' is punishable by jail time and fines), and India (with laws providing for extensive grounds for blockage or removal of harmful content and internet shutdowns).[101]

e. Oceania

In Oceania, there is no separate human rights treaty. But countries do have in place laws limiting harmful speech and online disinformation, including during elections. Australia, for instance, requires all "abhorrent violent material" to be blocked or removed.[102] Likewise, all paid electoral advertising, including on social media, to be authorized and to contain an authorization statement containing detailed financial information.[103] There are additional disclosure requirements for people and entities who undertake political or public communications activity in Australia on behalf of a foreign principal. Also in Australia, the Electoral Commission established protocols with Facebook and Twitter for the removal or blockage of posts that breach electoral advertising laws, or reporting details of their creators to the Commission[104] Australia also has established an Electoral Integrity Assurance Task Force to identify potential cyberattacks and foreign influence campaigns targeting its elections.[105]

98 Protection from Online Falsehoods and Manipulation Act 2019, No. 18 of 2019.
99 Computer Crime Act, B.E 2550 (2007); Thailand's Cybercrime Act Amendment (26 April 2016). See also here.
100 See here and here.
101 See here, here and here.
102 Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019, (Cth). See also here.
103 Electoral and Other Legislation Amendment Act 2017 (Cth) s 2.
104 See here.
105 See here.

V. Corporate Human Rights Standards

The concept of corporate responsibility to respect human rights rose to prominence following the publication of the 2011 Guiding Principles on Business and Human Rights, prepared by the Special Representative of the UN Secretary-General on the issue of human rights and transnational corporations and other business enterprises, Mr. John Ruggie.[106] Unlike a previous attempt to ground corporate responsibility in a 'non-voluntary comprehensive framework'[107] directly applying international human rights law to corporations,[108] the Ruggie principles speak of a (social) responsibility which exists outside the framework of directly binding international obligations. More recently, a UN Intergovernmental Working Group has made great strides towards the drafting of an international instrument on business and human rights. Both its 2018 Zero Draft[109] and 2019 Revised Draft[110] engage with the obligations of States vis-à-vis the operation of business enterprises. While the latest version of the draft legally binding instrument on the activities of transnational corporations and other business enterprises does not envisage the direct imposition of obligations on non-State actors, it does provide a comprehensive outline of the measures that States must adopt to ensure the undertaking of human rights due diligence by businesses.

The impetus for these initiatives is two-fold. First, it lies in the realisation that corporate actors can have an impact on the entire spectrum of internationally recognised human rights, and that this impact can materialise in the form of adverse consequences. In the Preamble of the Revised Draft, we read that

106 Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework.

107 Miretski and Bachmann, 'Global Business and Human Rights - The UN "Norms on the Responsibility of Transnational Corporations and Other Business Enterprises with Regard to Human Rights" - A Requiem'.

108 Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises with Regard to Human Rights, U.N. Doc. E/CN.4/Sub.2/2003/12/Rev.2 (2003). The Norms were met with criticism by both States and corporations, and the project of developing a framework for business and human rights found its new impulse in the work of John Ruggie.

109 For the draft treaty text and expert commentaries, see here.

110 The text of the revised draft is available here.

> … all business enterprises, regardless of their size, sector, operational context, ownership and structure have the responsibility to respect all human rights, including by avoiding causing or contributing to adverse human rights impacts through their own activities and addressing such impacts when they occur, as well as by preventing or mitigating adverse human rights impacts that are directly linked to their operations, products or services by their business relationships;

Second, it reflects a need for guidance – a need shared by both States and corporate actors – on the regulatory framework that States need to establish in order to discharge their own obligations under human rights law, and, by extension, on the standards that businesses should adopt in their operations. Even though a number of States have implemented legislation regulating the operations of businesses, and in particular online intermediaries, the standards are still embryonic and country-specific. In the absence of comprehensive standards, corporations have been active in developing their own standards and procedures. For instance, the Global Network Initiative (GNI), an alliance of Internet and telecommunications companies, human rights and press freedom groups, investors, and academic institutions has committed to implementing the GNI's Principles on Freedom of Expression and Privacy.[111] This initiative has been sounding the alarm bell on regulatory overreach by domestic authorities, recently in relation to the Brazilian Law of Freedom, Responsibility and Transparency on the Internet" bill.[112] It is important to note that the GNI does acknowledge the need to address online harms. Its criticism has been directed against particular types of regulation, for instance the requirements for pre-emptive filtering of some categories of content, especially where the benchmark itself is hard to delineate – as is the case with the term 'disinformation'.[113]

111 The GNI Principles are available here.

112 For a criticism of some of the provisions contained in the bill, see the Statement issued by the GNI here.

113 On 13 October 2020, the GNI released a policy brief on 'Content Regulation and Human Rights – Analysis and Recommendations', For a discussion on pre-emptive filtering of content, where it seeks to provide guidance on balancing tools to combat online harm with the perils of over-regulation, including impact on freedom of expression see here, p. 22.

Individual companies have also taken steps to address digital harms. Facebook, for instance, established an Independent Oversight Board tasked with the oversight of content moderation. In May 2020, it announced the first members and outlined a pathway for fleshing out the procedures of the Board within the ambit of a wide consultative process.[114] On content that could affect electoral processes more specifically, in September 2020 Facebook announced a set of steps it will take in order to protect the US election. Among the steps, we read a commitment to 'remove posts that claim that people will get COVID-19 if they take part in voting' and to 'attach a link to authoritative information about the coronavirus to posts that might use COVID-19 to discourage voting'.[115] More recently, Facebook announced that, to safeguard the 2020 election in Myanmar, it will, inter alia, demote likely hate speech, expand misinformation labels to the Burmese language, and direct people to authoritative voting information.[116]

But difficult questions remain. One primary concern with the imposition of corporate standards that may curtail freedom of expression online is the prospect of a decision-making process lacking legitimacy. In particular, the lack of transparency of all processes leading to the adoption of Terms of Service, Codes of Conduct, and other documents regulating digital content could be seen as problematic when these standards directly affect the enjoyment of rights online. Another concern is one of reach: how far should States allow corporate actors to restrict the types of speech on their platforms? According to Kate Jones, while this question is still unsettled, standards may differ across companies. For instance, there could be differentiated regulation between a small online intermediary and platforms such as Facebook or Twitter that have come to play a crucial role in enabling and facilitating conversations on matters of public interest.[117]

114 Nick Clegg, Welcoming the Oversight Board (6 May 2020).
115 The announcement made by Mark Zuckerberg is available here.
116 For the full set of steps, see here.
117 Chatham House, Online Disinformation and Political Discourse: Applying a Human Rights Framework (2019) Research Paper prepared by Kate Jones, p. 29.

VI. Conclusion: new challenges for the protection of human rights in the digital space

While it is recognised that human rights need to be protected both offline and online, their protection in those environments may vary significantly. Online platforms pose new and significant challenges, as they allow information to spread at an unprecedented scale and speed. This means that the measures States must adopt to discharge their human rights obligations, including the type of restrictions imposed on free speech, may depart from those applicable to traditional media outlets.

One particular challenge is that even the regulatory schemes in place on the regional and domestic level may prove to be inefficient when faced with concerted large-scale political disinformation campaigns. The German and French laws on content moderation, which have already been criticised for their wide-ranging and potentially chilling effects, may be well-suited for content take-downs in cases of isolated individuals posting harmful content that are then subjected to platform review. However, these may be inadequate for the type of automated, large-scale generation of content by fake accounts or bots.

Existing jurisprudence is also still dealing with disinformation in a more traditional form. In Brzeziński v. Poland, the ECtHR explicitly refers to the phenomenon of 'fake news. Yet it does so in the context of local elections in Poland and a statement made by a candidate for a local government position towards the outgoing local administration. The Court recognised the necessity of combatting the dissemination of false information on electoral candidates in view of retaining the integrity of the public debate.[118] It then examined the traditional elements for consideration, including the context of a debate on public interest, the position of the applicant in that debate, the harm inflicted, and reiterated that there is little scope for restrictions on political speech. In that case, the Court did not find evidence that the national authorities

118 Brzeziński v. Poland, ECtHR, Judgment of 25 July 2019, para. 55.

had considered whether the applicant's remarks had a factual basis and whether he had acted with the requisite diligence. It remains to be seen how and whether these principles could be tailored to new contexts where the purposeful spread of false or manipulated information forms part of large-scale orchestrated operations, with some users unknowingly sharing harmful content and thus magnifying its reach and effect. It also remains to be seen whether positive obligations stemming from the right to seek and impart information, freedom of thought and opinion, the right to participate in public affairs and to vote, and the right to privacy could require States to take specific measures to tackle such campaigns.

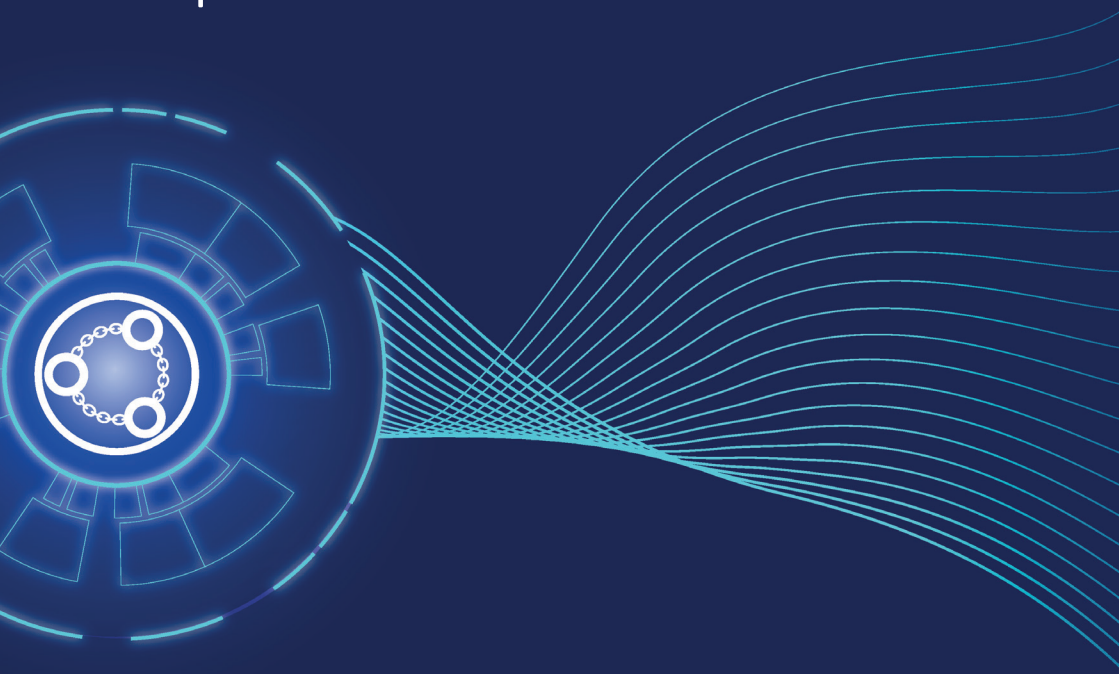
In sum, while the existing human rights law frameworks are capable of addressing the phenomenon of online electoral disinformation, the specific standards that guide us on the scope of the rights at stake, the reach of the State obligations these rights give rise to, and the necessity and proportionality of the restrictions may be in need of further clarification and development.

4 The Oxford Process on International Law Protections in Cyberspace: The Protection of IT Supply Chains under International Law

'The Oxford Process has been a valuable forum for dialogue between legal practice and academia. It is now widely accepted that international law applies to cyber operations, but the Oxford Process has pioneered the inevitable next step in that discussion: a frank and open exchange of views about how exactly international law might protect our societies from different types of harmful cyber activities. Wherever those discussions exposed differences in legal reasoning, the pragmatic format of the Oxford Process encouraged participants to strive for shared conclusions around internationally wrongful behaviours in cyberspace. The inventive use of video conferencing and hybrid meetings also extended the discussions to a diverse, global audience, straddling continents, time zones and respective legal traditions, thereby ensuring a fully inclusive expert process.'

Shehzad Charania MBE,
GCHQ Director of Legal Affairs and International Relations

Virtual workshop
Report



The Oxford Process on International Law Protections in Cyberspace:

The Protection of IT Supply Chains under International Law

16 March 2021

Executive Summary & Key Takeaways

On March 16th, 2021, the Oxford Institute for Ethics, Law and Armed Conflict (ELAC) held a virtual workshop, sponsored by Microsoft, on the regulation of IT Supply Chains. This workshop was part of the Oxford Process on International Law Protections in Cyberspace, an initiative seeking to identify points of consensus on international legal rules and principles in their application to specific sectors, objects of protection and methods employed by different cyber operations. This workshop was the fourth one in the Oxford Process series, following on from two events focused on the protection of the healthcare sector (May 2020 on the healthcare sector in general, and July 2020 on the protection of vaccine research) and one on the regulation of foreign digital interference in electoral processes (October 2020).

With the SolarWinds hack as its immediate catalyst, the workshop examined the range of international rules relevant to the protection of IT supply chains. The main focus of the event was on the following two overarching questions: (1) whether the characterisation of an operation as 'espionage' precludes a finding of breaches of other rules of international law, such as the rules of non-intervention and sovereignty, human rights obligations, the Corfu Channel and no-harm principles; (2) what is the scope of these rules of international law, and how they apply to the protection of IT supply chains.

There was widespread agreement among the participants on the following points:

1. Cyber operations against IT supply chains pose unique challenges. This is due, inter alia, to their indiscriminate effects and the undermining of trust in systems that are regarded as essential for the operation of the internet.

2. International law applies to information and communication technologies (ICTs), including to cyber operations against IT supply chains.

3. The qualification of an operation as 'espionage' does not preclude a finding that such an operation may be in violation of international law because of its means, method or effects.

4. It is critical to specify the scope of the relevant international legal rules and principles as they apply to ICTs. Outstanding controversies around the principles of sovereignty and non-intervention, the Corfu Channel and no-harm rules, and the scope of 'jurisdiction' under international human rights law treaties, among others, continue to pose challenges to legal certainty and may have adverse consequences for the deterrent effect of these rules and principles.

5. Further study on the regulation of the means, methods and effects of cyber operations is required.

Background

On March 16th, 2021, the Oxford Institute for Ethics, Law and Armed Conflict (ELAC) held a virtual workshop, sponsored by Microsoft, on the regulation of IT Supply Chains. This workshop was the fourth in the Oxford Process on International Law Protections in Cyberspace series, following on from two events focusing on the protection of the healthcare sector (May and July 2020) and one on the regulation of foreign digital interference in electoral processes (October 2020).

Just as with previous Oxford Process events, the March workshop was prompted by pressing concerns over the intensification of particular types of cyber activity. On this occasion, these concerns were related to operations against IT supply chains, with the recent SolarWinds hack as a striking example and reference point for the discussions. As legal, policy and IT circles were learning more about the operation, its method, direct effects and broader implications, one important question started to dominate domestic and international conversations: was the SolarWinds operation 'mere' espionage? The workshop sought to move past the espionage label and inquire into the possibility of such operations breaching international law because of its means, methods or effects. In particular, the workshop focused on the following two overarching questions: (1) whether the characterisation of an operation as 'espionage' precludes a finding of breaches of other rules of international law, such as the rules of non-intervention and sovereignty, human rights obligations, the Corfu Channel and no-harm principles; (2) what is the scope of these rules of international law, and how they apply to the protection of IT supply chains.

Summary of Sessions

Welcome and Introduction

Professor Dapo Akande (ELAC) and Professor Duncan B. Hollis (Temple University) gave the introductory remarks. Professor Akande clarified the goal of the Oxford Process, which is to effectuate a transition from the debates on the applicability of international law to ICTs to a conversation on the specification of legal rules in this context. Moving beyond the statement that international law applies to ICTs, the Process seeks to examine how exactly it applies. The approach taken by this initiative, unlike the Tallinn Manuals and the meetings of the Open-Ended Working Group on Information and Communication Technologies, is to look at specific types of activities, such as cyber operations targeting the healthcare sector, vaccine research, digital electoral interference, and information operations and activities. Professor Hollis emphasised that the goal of the

Oxford Process is to identify commonalities. Previous Oxford Statements have shown that more than a hundred lawyers can agree on a range of challenging legal questions.

The workshop was organised around three sessions. The first one was aimed at providing an overview of the SolarWinds and Microsoft Exchange hacks, thus introducing the participants to the landscape of threats and types of vulnerability exploitations in the supply chain the IT community had been observing in the past months. The second session considered whether there is or ought to be international law that applies specifically to espionage and cyber espionage. The third session, leaving the legal regulation of espionage aside, examined the possible application of other rules of international law to such cyber activities, even if the aim of the activity can be qualified as espionage.

Session I

The SolarWinds Hack: What do we Know?

Speaker: Tom Burt, Corporate Vice President, Customer Security & Trust, Microsoft

This session focused on the methodologies leveraged in recent IT supply chains operations, and the implications for the IT sector and its users. At the outset, Mr Burt noted that the cyber operations observed, both recently and in the past with Stuxnet, NotPetya or WannaCry, show the potential destructive power of offensive cyber operations. Their effects highlight the need to work towards the clarification of rules of international law and, if international law is found to lack adequate and sufficient protections, towards filling the relevant gaps through new rules and norms.

The SolarWinds hack, perpetrated by a nation-State actor operating from Russia, leveraged a sophisticated technique to infiltrate the network of a small software company called SolarWinds. SolarWinds have a popular application called Orion, which is used to optimize network performance. It is most likely that the actor entered the company's environment

through password spraying. Once the intrusion was successful, the perpetrators had to wait for an update to the Orion software. At that point, malware was incorporated into the build, signed with the SolarWinds' digital certificate. The updated was applied by 33,000 customers globally and about 18,000 in the US between March and June 2020 alone and all of these customers unknowingly installed the malware. Once in the customers' systems, the malware remained there quietly at first to avoid detection. As it was not placed into the source code tree, detection at this stage was particularly challenging. Later it navigated to the command-and-control server, which allowed hackers to move through the users' networks, seeking credentials of network administrators. They used a variety of techniques to gain escalated privileges within those networks, stealing significant amounts of data. At this stage, the perpetrators utilized second-stage malware and closed the initial backdoor to cover their tracks. Had the attackers stayed entirely on premise, they may have remained undiscovered. However, they also created identities that allowed them to access cloud services. Fortunately, FireEye discovered their presence in their network: the anomalous use of cloud services allowed the detection of small digital footprints.

Mr Burt noted that state actors have been compromising supply chains for espionage purposes for a number of years. What was unique about the SolarWinds attack was the sophisticated use of a technique pioneered in the NotPetya attack – the compromise of a security update. However, with NotPetya, perpetrators used ransomware to shut down the digital ecosystem of key Ukrainian service providers. This, in turn, caused significant disruption to the life of Ukrainians, as well as significant global economic fallout.

Mr Burt also addressed the Microsoft Exchange Server data breach. Four vulnerabilities in the on-premises Exchange server were targeted by an actor operating from China. A day before Microsoft was meant to issue a patch for the vulnerability, they saw a sudden escalation in the latter's exploitation. Learning about the patch, these actors orchestrated

a campaign to compromise as many networks as they could. The methods of these attacks, according to Mr Burt, pose interesting questions about the actors behind them. Ransomware operators do not typically engage in attacks that are expensive and challenging. Both the SolarWinds and Microsoft Exchange breaches were difficult, time-consuming and expensive to carry out.

In his final comments, Mr Burt emphasized the need to prevent such software update attacks. Update processes have to be trusted by customers. If customers cease to trust the process, companies cannot keep them secure. This is precisely why these attacks were particularly insidious.

During the discussion, one participant enquired whether the unique nature of these attacks can be summarized along three benchmarks: nature, purpose and effect. Their nature would be compromising IT supply chains to enter the system, their intent – proliferation at a very grand scale, not just to engage in targeted intervention for espionage, but to achieve much broader infiltration – and their effect being to cast doubt on the integrity of the software infrastructure. This final point raised concerns over the high potential not just for immediate, but also for long-term harm. According to Mr Burt, it is the corruption of the update process that made these operations unique and problematic. If the actors can successfully place the malware in the build process, they get the advantage of the company's digital signature. This, of course, could have a catastrophic impact in cases where the victims are critical infrastructure providers. On intent, regardless of the aim of the attacker, which may be quite narrow, the technique used had a very wide blast radius. Mr Burt reiterated that, in his view, the compromise of a vendor's update process should be inherently a violation of international law, at least for a vendor who has international customers. Customers' trust in the update process is so fundamental to the security of the digital ecosystems that States should not be allowed to compromise such processes.

Session II

Beyond the Narrative of Silence: International Law and Cyber Espionage Operations

Speaker: Naomi Hart, Essex Court Chambers

Dr Hart's presentation sought to clarify whether international law imposes any constraints on espionage activities. As noted by Dr Hart, espionage remains a ubiquitous feature of international relations. This, however, was not considered as entailing that it is a constraints-free space. Despite any perceived urgency over the protection of IT supply chains, it has to be borne in mind that the formation of rules of customary international law is an accretive process. Identification is a time-consuming forensic exercise. Dr Hart emphasised the need to ensure that no short-cuts are being taken just because of the urgency of the facts on the ground. The issue of the legality of activities falling under the heading of espionage can arise for governments, if they are considering countermeasures as a response (as countermeasures require prior illegality), for an international court, such as the International Court of Justice (for instance, under a compromissory clause in a treaty, such as the Vienna Convention on Diplomatic Relations), or for domestic courts. In all these contexts, Dr Hart opined, a black-letter positivist approach would be required.

The following points on the legal analysis of espionage activities were made by Dr Hart:

International law has clear tools for identifying rules of customary law, and it contains a series of presumptions we can fall back on if no customary rule can be found to exist. The starting point is that States can act as they see fit in the absence of a specific prohibition. It would be really difficult to say that, as international law currently stands, States have coalesced around a view that inter-State intelligence-gathering is prohibited. One of the barriers in the identification exercise is that espionage by definition occurs in secret. It is unclear how many States carry out such operations, with what intensity and in what form. While

it may be clear that certain States do engage in espionage (the UK, US and Israel, for instance), this does not provide an inclusive view of State practice. Discerning *opinio juris* may be even more challenging. The fact that States spy does not automatically mean that they accept they have a right to do so. Similarly, not spying does not mean that the practice is illegal. As far as we can tell from State practice and *opinio juris*, it is not possible to conclude that there is a rule of international law prohibiting States from engaging in espionage per se. This, however, is not the end of the analysis. Other rules of international law may constrain or positively authorise espionage in certain contexts. The difficulty that arises here is around the specification of these rules, as the scope of many of them is still heavily contested.

Discussant: Gary Corn, Director, Technology, Law & Security Program, American University Washington College of Law

The first discussant, Professor Corn, emphasised the importance defining of our starting point: are we discussing whether SolarWinds itself was a violation of international law, or whether supply chain attack methodologies more broadly are a violation of international law, or whether espionage is inconsistent with international law in whole or in part? Framing the discussion is crucial. According to Professor Corn, supply chain attacks are a methodology, and that methodology is not new. Operations against IT supply chains are not the same in every circumstance and must be assessed separately for each operation. We are now observing a shift from traditional espionage, which was much more targeted and focused, to a situation where an attacker can broaden the target set, and where the cost to gathering data is lower. The concerns here are different, both as to the potential scope and scale of IT supply chain operations and the risk they pose of collateral impacts. Depending on the data being taken, such operations also implicate privacy in different ways. In the opinion of Professor Corn, the most useful question may be whether the law needs to change. He agreed with Tom Burt that this is a moment for condemnation. But what the frame for that condemnation should be, he opined, is a matter to be considered carefully.

Discussant: Asaf Lubin, Associate Professor of Law, Indiana University Maurer School of Law

The second discussant on this panel, Dr Lubin, advanced five key points for the consideration of the participants. First, he argued that a stringently formalistic and positivist account of the international law of intelligence should be rejected. Rather, we should adopt context, process and value-based interdisciplinary viewpoints focusing on the function intelligence plays in public world order. Only then can we appreciate espionage qua espionage. He further advanced the view of the existence of a lex specialis of intelligence: a body of special secondary rules, institutions and enforcement mechanisms governing inter-state espionage. Second, the discussant opined that States enjoy a liberty to engage in peace-time intelligence operations under existing customary international law. This liberty was seen as a pre-requisite for the existing security system. Third, further customary rules surrounding foreign intelligence operations can emerge over time. Since the end of the Cold War and certainly after the Snowden revelations, we have ushered in an era of "intelligence legalism," where States are legally defending their activities and collaborating with partners in far more public ways. Fourth, internationalists have developed an obsession with sovereignty that may be antiquated, as advocating solely for territorial line-drawing in the regulation of cyberspace seems out of touch. Fifth and finally, the regulation of intelligence occurs at three distinct temporal stages: before, during and after an operation. For each phase, different rules and principles apply. We should consider a set of general principles of law, legality, necessity, effectiveness, proportionality, adequate safeguards, good faith, and fairness in assessing particular operations. These principles could either apply as customary human rights obligations or as a standalone Article 38(1)(c) source. Rule-appliers should thus examine the legality of SolarWinds in light of these principles.

The moderator of this session, Professor Akande, framed the discussion by inquiring into the significance of making the claim that a certain operation constitutes espionage. Such a claim could be significant in a

number of ways. First, it could be claimed that, because it is espionage, there is a different legal framework that applies. Second, it could be argued that because States engage in espionage, they have a right to do so, and no further questions of legal restraints are to be asked.

According to some participants, to fully understand the regulation of such operations, we need to disaggregate them, and consider the differences between economic and political espionage, with a potential finding that economic espionage is prohibited under international law. Other participants were not convinced that there is sufficient consensus to say that espionage for economic purposes is unlawful.

During the discussion, some participants noted the qualitative evolution of espionage operations. Previously, actors sought to hide knowledge of their activities from the public view. Now, as shown by the DNC hack, the objective is often to release the stolen records at a time calculated to have maximum political impact.

A central question in the discussion was that of prevention. In the absence of a consensus over norms of restraint, and yet in the presence of so many clashes of interests over norms of restraint, why would adversaries stop their pernicious activities and how can they be convinced to stop? It was noted that norm-transgressors have every interest in preventing the clarification of rules, and the development of new rules to govern this space. Relatedly, one interpretation given to the Microsoft Exchange hack was that the actors sought to show that this is an activity they can freely engage in. Participants agreed that rules need to be clear if we expect States to follow a certain type of conduct.

There was widespread agreement that the label espionage does not preclude a finding of a violation, where the means, methods and effects of espionage operations fall foul of international legal rules. According to some, that regulation of means, methods and effects exists only at the outer boundaries of what our concerns regarding IT supply chains

operations are. For the SolarWinds hack, some participants considered that we can discern a clear vulnerability vector, which may allow a finding of illegality on the means, methods or effects plane. An analogy with armed conflict was drawn: while parties to a conflict may have a right to target certain objectives, there are limitations on the ways that the targeting can occur. In the context of IT supply chain operations, some considered that tainting the entire supply chain may not be an accepted methodology.

For some participants, the discussion showed that international law, as it currently stands, is insufficient to meet our protection needs and has to evolve. To achieve incremental change, this change needs to be seen as building on processes that are familiar to the audience.

Session III

International Law and the Protection of IT Supply Chains

Speaker: Russell Buchan, Senior Lecturer in International Law, University of Sheffield

Despite the lack of specific regulation of espionage under international law, Dr Buchan's argument in his presentation was that international law does have a set of rules and principles that can constrain operations classified as espionage. These rules come from a variety of fields, including international human rights law, international economic law and diplomatic law. It is critical, he argued, to identify the place or location from which espionage occurs (from a national territory or outer space, for instance); who the responsible actor is (State or non-State actor); and the type of information collected (critical information or trade secrets of a private company).

According to Dr Buchan, territorial sovereignty is a rule that is of particular relevance in this space. It is a rule that permits States to exercise governmental functions free from interference. Just as non-consensual trespass in State territory in the physical world is seen as a clear violation of the principle, operations that 'trespass' into sovereign

cyber territory should be seen as breaching the law. The principle should be divorced from the idea of harm and damage. For instance, focusing on operations requiring significant remedial action would bring additional challenges, as this requirement would make the application of the principle more subjective. By divorcing the rule from these requirements, we would more closely align with its application in the physical world, and also give it a more meaningful scope in cyberspace.

Discussant: Kristen Eichensehr, Martha Lubin Karsh and Bruce A. Karsh Bicentennial Professor, University of Virginia School of Law

The first discussant, Professor Eichensehr, in responding to Dr Buchan's remarks, noted that the state of play is quite mixed with respect to the rule on sovereignty: quite a few States do not (or not yet) recognise territorial sovereignty as a standalone rule. Even States recognising it do not necessarily agree on its scope. A number of states that recognise sovereignty as a rule have announced a threshold requirement – a level of harm or effects that must be surpassed before the rule is violated. Professor Eichensehr opined that a crucial question concerns the risk levels States are ready to accept. If states cannot or will not restrict espionage per se, should we instead focus on preventing disruption? In other words, even if international law rules do not stop espionage, can they stop escalation? Focusing on attempting to stop disruptive intrusions rather than all intrusion may give other international law rules, particularly the prohibition on intervention a greater role to play. Anumber of states have recently moved to provide greater clarity about their views on the scope of the prohibition on non-intervention, though the boundaries of this rule too remain disputed and fuzzy. And, finally, Professor Eichensehr noted that States have not failed to regulate espionage; rather, they have done so in their domestic systems through criminalisation and tools for enforcement. Domestic regulation may have an impact on individual deterrence, and it could also render espionage less effective and less disruptive by mandating better defenses.

Ciaran Martin, Professor of Practice, Blavatnik School of Government, University of Oxford

Professor Martin, the second discussant in this session, emphasised the need to keep these legal assessments close to the operational reality of how States see such operations. He agreed with the scepticism around territorial sovereignty as a rule expressed by the first discussant. Thinking about the future steps of the Oxford Process, he suggested tying the legal discussion to geopolitical imperatives and acknowledging that espionage can sometimes have a useful function.

In the open discussion, participants highlighted several areas of law that have relevance for the regulation of operations impacting IT supply chains. Many participants considered international human rights law to be a fruitful avenue for thinking about the impact of such operations, as individuals can find themselves to be their intended or unintended targets. Particular rights discussed were privacy, health, life, expression and property. It was noted that the main challenge facing such claims under international human rights law is the controversy over the extent of extraterritorial jurisdiction. The importance of discussing the responsibility of businesses to respect rights was also highlighted by some participants.

Related to the transition from a perpetrator's perspective to a victim's perspective, the moderator, Professor Hollis, noted the significance of remaining mindful of the externalities and spill-over that operations such as SolarWinds cause. These externalities and spill-over effects are connected to a broader discussion on the risks and threats inherent in IT supply chain attacks using the methods recently observed. One participant noted that these risks and threats were highlighted in the 2021 OEWG Report.

On the point of lex ferenda, some participants raised the possibility of fleshing out rules that protect the public core of the internet.

Concluding remarks

At the end of the session, Professor Akande identified some of the commonalities discerned during the discussion.

First, it seems that the most serious concern is over operations that damage trust in systems that are regarded as essential for the operation of the internet. The question, then, is whether there are any legal rules that constrain cyber operations against such systems. A potential obstacle to articulating these rules is that the operations are often conducted for the purpose of espionage.

Second, the purpose of espionage raises a new host of questions: is there special regulation of espionage under international law? Is there a right to engage in espionage? There seemed to be broad consensus that simply labelling something 'espionage' does not mean there is a lack of legal regulation, i.e. the label does not place the operation beyond international regulation.

Third, there is a need to look deeper at the means, methods and effects of operations. The relevant principles and rules – sovereignty, international human rights and others – are in need of further specification.

List of Workshop Participants

1) Christiane Ahlborn, Legal Officer, UN Office of Legal Affairs
2) Dapo Akande, Professor of Public International Law, Co-Director, Oxford Institute for Ethics, Law & Armed Conflict (ELAC), University of Oxford
3) Leonie Arendt, Policy Consultant, UN Foundation
4) Karine Bannelier-Christakis, Associate professor of International Law, Université Grenoble Alpes
5) Nayia Barmpaliou, Non-Resident Expert, Cybersecurity, European Union Institute for Security Studies
6) Russell Buchan, Senior Lecturer in International Law, University of Sheffield
7) Tom Burt, Corporate Vice President, Customer Security & Trust, Microsoft
8) Scott Charney, Vice President, Security Policy, Microsoft
9) Kaja Ciglic, Senior Director, Digital Diplomacy, Microsoft
10) Antonio Coco, Lecturer in Public International Law, University of Essex and Visiting Fellow at ELAC, University of Oxford
11) Gary Corn, Professor of Law and Director of Technology, Law & Security Program, American University Washington College of Law
12) Enrico Cossidente, Italian Army staff officer and military legal advisor
13) Jennifer Daskal, Deputy General Counsel, US Department of Homeland Security
14) Francois Delerue, Research Fellow in Cyberdefense and International Law, Institute of Strategic Research of the Military Academy, France
15) Miguel de Serpa Soares, Under-Secretary-General for Legal Affairs and United Nations Legal Counsel
16) Talita Dias, Research Fellow, Jesus College & ELAC, University of Oxford
17) Kristen Eichensehr, Martha Lubin Karsh and Bruce A. Karsh Bicentennial Professor of Law, University of Virginia
18) David Fidler, Adjunct Senior Fellow for Cybersecurity & Global Health, Council on Foreign Relations
19) Naomi Hart, Barrister, Essex Court Chambers
20) Duncan B. Hollis, Laura H. Carnell Professor of Law, Temple University School of Law
21) Zhixiong Huang, Professor of International Law & Vice Dean for International relations, Executive Director, Wuhan University Institute for Cyber Governance, Wuhan University

22) Graham Ingram, Chief Information Security Officer, University of Oxford
23) Katie Johnston, DPhil candidate in International Law, University of Oxford
24) Kate Jones, University of Oxford
25) Andraz Andy Kastelic, Lead cyber stability researcher, Security and Technology Programme, UNIDIR
26) David Kaye, Clinical Professor of Law, University of California, Irvine
27) Lucas Kello, Associate Professor of International Relations, University of Oxford
28) Harold Hongju Koh, Senior Adviser and former Legal Adviser (2009-13), Office of the Legal Adviser, US Department of State
29) Jeffrey Kovar, Assistant Legal Adviser for Political-Military Affairs, US Department of State
30) Leonhard Kreuzer, Research Fellow, Max Planck Institute for Comparative Public Law and International Law
31) Joanna Kulesza, Professor of Law, University of Lodz
32) Masahiro Kurosaki, Associate Professor of International Law and Director of the Study of Law, Security and Military Operations, National Defense Academy of Japan
33) Grace L, GCHQ
34) Henning Lahmann, Senior Researcher, Digital Society Institute, ESMT Berlin
35) Marja Lehto, Ambassador and Senior Legal Expert, Minister of Foreign Affairs, Finland
36) Asaf Lubin, Associate Professor of Law, Indiana University Maurer School of Law
37) Kubo Mačak, Legal Adviser, International Committee of the Red Cross, Associate Professor, University of Exeter
38) Nemanja Malisevic, Director, Digital Diplomacy International Lead, Defending Democracy Program, Microsoft
39) Ciaran Martin, Professor of Practice, Blavatnik School of Government, University of Oxford
40) Tomohiro Mikanagi, Deputy Director-General of the International Legal Affairs Bureau, Ministry of Foreign Affairs of Japan
41) Tomáš Minarik, Head of International Organisations and Law Unit, National Cyber and Information Security Agency of the Czech Republic
42) Harriet Moynihan, Senior Research Fellow, International Law Programme, Chatham House
43) Jan Neutze, Senior Director, Digital Diplomacy, Microsoft
44) Kazuho Norikura, Ministry of Foreign Affairs, Japan

45) Jim O'Brien, Vice Chair, Albright Stonebridge Group
46) Giacomo Persi Paoli, Programme Lead for Security and Technology Programme, UNIDIR
47) Patryk Pawlak, Executive Officer, European Union Institute for Security Studies
48) Przemysław Roguski, Lecturer in Law, Jagiellonian University in Kraków
49) Vera Rusinova, Professor of International Law, Higher School of Economics in Moscow
50) Michael Schmitt, Professor of International Law, University of Reading; Francis Lieber Distinguished Scholar at the Lieber Institute of the United States Military Academy (West Point)
51) Corinna Seiberth, Lawyer, Federal Department of Foreign Affairs FDFA, Directorate of International Law, International Law Division, Switzerland
52) Nicola Smith, Legal Counsellor and Head of the National Security Team, FCDO
53) Marcus Song, Senior State Counsel, International Affairs Division, Attorney-General's Chambers, Singapore
54) Hansjoerg Strohmeyer, Chief of Policy Development and Studies Branch, United Nations Office for the Coordination of Humanitarian Affairs
55) Nikhil Sud, Regulatory Affairs Specialist, Albright Stonebridge Group
56) Masaru Suzuki, First Secretary, Embassy of Japan in the United Kingdom
57) John Swords, Legal Adviser and Director of the Office of Legal Affairs at NATO Headquarters
58) Wieteke Theeuwen, Legal Officer, International Law Division, Ministry of Foreign Affairs of The Netherlands
59) Tsvetelina van Benthem, Research Officer, ELAC
60) Liis Vihul, Chief Executive Officer, Cyber Law International
61) Marguerite Walter, Attorney-Adviser, Human Rights and Refugees, Office of the Legal Adviser, US Department of State
62) Alexander Wentker, DPhil candidate in International Law, University of Oxford
63) Stephen Wheatley, Professor of International Law, University of Lancaster
64) Robert Young, Legal Counsel, Global Affairs Canada

Espionage and Elusive Rules of Customary International Law

*Naomi Hart**

*Dr Naomi Hart is a barrister at Essex Court Chambers. She attained a doctorate from the University of Cambridge on the topic of espionage and public international law, for which she was awarded the Faculty of Law's Yorke Prize.

Introduction

History is replete with examples of sensational disclosures of highly invasive intelligence operations by one State against another. Even as part of this long catalogue, the SolarWinds hack which was uncovered in late 2021 stands out for the apparent degree of penetration it achieved, its longevity prior to discovery by its targets, and the scale of its effects for not just public but also private actors. It has rightly prompted reflection on whether current rules of international law are adequate to protect information concerning complex supply chains from malicious covert intelligence collection.

The need for immediacy in responding to the SolarWinds hack stands in stark contrast to the accretive, typically slow, process by which rules of customary international law form. Despite espionage being a practice as old as diplomacy itself, the international community has never reached any sort of consensus on the legality of this ubiquitous activity. This paper tackles a simple question: why is it so hard to identify rules of customary international law that regulate inter-State espionage *per se*, as opposed to espionage as a manifestation of conduct that is captured by more widely applicable rules of international law?

The international lawfulness of covert intelligence activities between States is hotly contested by scholars. Some authors assert a customary prohibition on intelligence gathering.[1] Others, at the extreme opposite end of the spectrum, assert that there is a "right" to spy,[2] implying not simply that

1 See, e.g., Richard R Baxter, "So-called 'Unprivileged Belligerency': Spies, Guerrillas and Saboteurs" (1951) 28 BYBIL 323, 329; Quincy Wright, "Espionage and the Doctrine of Non-intervention in Internal Affairs" in Roland J Stanger (ed), Essays on Espionage and International Law (Ohio State University Press 1962) 3, 12; Ingrid Delupis, "Foreign Warships and Immunity for Espionage" (1984) 78 AJIL 53, 67; 408.
2 See, e.g., Thomas C Wingfield, The Law of Information Conflict: National Security Law in Cyberspace (Aegis Re-

espionage is internationally permissible by default in the absence of a prohibition, but also that customary international law embodies a positive permission to spy that may render such conduct lawful even in situations where it would otherwise be prohibited. A sizeable scholarly contingent implies that covert intelligence gathering is of indeterminate legality as a matter of customary international law or even eludes customary international legal regulation entirely. A favourite term of such writers to describe the customary position on espionage is "ambivalent".[3] Other authors claim that, when it comes to covert intelligence collection, customary international law is "agnostic[]",[4] "curiously ill-defined",[5] "silent",[6] "unrecognized",[7] "virtually unstated",[8] or "remarkably oblivious";[9] that customary international law "neither endorses nor prohibits espionage",[10] or simply "ignores" it;[11] or that espionage exists in a "lacuna", "penumbra", "peculiar limbo" or "gray zone" within customary international law.[12] Some authors have gone so far as to doubt whether international law plays any actual or potential role in governing espionage.[13]

search Corp 2000) 350; David M Crane, "Fourth Dimensional Intelligence: Thoughts on Espionage, Law, and Cyberspace" (2002) 76 Intl Leg Stud Series—US Naval War College 311, 312; Jeffrey H Smith, "Symposium on State Intelligence Gathering and International Law: Keynote Address" (2007) 28 Mich JIL 543, 544; Glenn Sulmasy and John Yoo, "Counterintuitive: Intelligence Operations and International Law" (2007) 28 Mich JIL 625, 628.

3 Sean P Kanuck, "Information Warfare: New Challenges for Public International Law" (1996) 37 HILJ 272, 276; A John Radsan, "The Unresolved Equation of Espionage and International Law" (2007) 28 Mich JIL 595, 596; Dieter Fleck, "Individual and State Responsibility for Intelligence Gathering" (2007) 28 Mich JIL 687, 708; Catherine Lotrionte, "Countering State-Sponsored Cyber Economic Espionage under International Law" (2015) 40 NCJIL Comm Reg 443, 475.

4 Ashley Deeks, "An International Legal Framework for Surveillance" (2015) 55 VJIL 291, 319.

5 Christopher D Baker, "Tolerance of International Espionage: A Functional Approach" (2004) 19 American University Intl LR 1091, 1094.

6 Richard A Falk, "Foreword" in Roland J Stanger (ed), Essays on Espionage and International Law (Ohio State University Press 1962a) v, v; G N Barrie, "Spying—An International Law Perspective" [2008] J South African L 238, 238.

7 Leslie S Edmondson, "Espionage in Transnational Law" (1972) 5 Vanderbilt J Transnatl L 434, 436.

8 Geoffrey B Demarest, "Espionage in International Law" (1996) 24 Denver JILP 321, 321; Chantal Khalil, "Thinking Intelligently about Intelligence: A Model Global Framework Protecting Privacy" (2015) 47 Geo Wash Intl LR 919, 921.

9 Falk (n 6) v (cited with approval in Radsan (n 3) 602; Khalil (n 8) 927).

10 Baker (n 5) 1092. See also Raphael Bitton, "The Legitimacy of Spying among Nations" (2014) 29 American University Intl LR 1009, 1057 ("espionage seems to be both legal and illegal at once").

11 Demarest (n 8) 339; Christina Parajon Skinner, "An International Law Response to Economic Cyber Espionage" (2014) 46 Conn LR 1165, 1182; Lotrionte (n 3) 473.

12 Skinner (n 11) 1182; Simon Chesterman, "The Spy who Came in from the Cold War: Intelligence and International Law" (2006) 27 Mich JIL 1071, 1130; Lotrionte (n 3) 475; Howard J Taubenfeld, "The Status of Competing Claims to Use Outer Space: An American Point of View" (1963) 57 ASIL Proc 173, 132.

13 Falk (n 6) vi; Radsan (n 3) 596; Sulmasy and Yoo (n 2) 626.

Few — if any — of these scholars have undertaken the sort of rigorous analysis of State practice and *opinio juris* which would yield a cogent conclusion on whether customary international law specifically forbids or positively authorises espionage, and on the rules that apply in the absence of a specific prohibition or permission. This paper seeks to both explain and correct what it sees as this methodological shortcoming in previous research. First, it identifies characteristics of espionage that mean that an analysis of State practice and *opinio juris* does not uncover a positive rule either permitting or proscribing espionage per se. Secondly, it discusses certain international legal consequences that flow from an absence of such specific rules, including the engagement of other rules of international law to govern espionage in certain forms. In its conclusion, it suggests that States' competing and inconsistent interests in the legality of espionage are likely to sustain a status quo in which this practice escapes specific international legal regulation.

Ascertaining rules of customary international law specific to espionage

Employing an orthodox positivist methodology, the legality of espionage under customary international law should be determined by gathering evidence of relevant State practice and *opinio juris*. A purported customary rule authorising certain conduct must be supported by the sufficient (and sufficiently representative) practice of States acting in conformity with it, and then only if that practice is carried out in the belief on the part of the same States that it is either permitted or required by customary international law. Likewise, in order to support a rule of custom prohibiting a certain conduct, protest against or abstention from that conduct must be accompanied by the belief that the conduct is unlawful as a matter of customary international law, rather than merely undesirable.

When it comes to establishing whether there exists a specific customary prohibition or permission relating to espionage, multiple empirical and

doctrinal difficulties present themselves. This paper addresses just two of these difficulties.

First, the secrecy with which espionage is conducted poses both an issue of principle and a practical challenge to marshalling evidence. There is little publicly available, detailed information about the objectives, operations, capabilities or assessments of national intelligence agencies — for the obvious reason that, the less that is publicly revealed, the more effectively such agencies can operate.

The clandestine character of espionage raises a preliminary analytical question as to whether State practice that occurs secretly can contribute to the formation of rules of customary international law. Commentators adopt different positions on this question. Some claim that conduct does not 'count' as State practice unless it has been publicised on the basis that other States lack an opportunity to respond to such conduct.[14] This claim is, however, difficult to reconcile with the inclusive view of State conduct that qualifies as practice capable of supporting a customary norm. Covert acts do not possess a different legal quality to overt acts. The lack of opportunity for other States to respond to those acts may diminish the quantity of State practice and opinio juris available in the assessment of their legality, but does not, in principle, exclude them from consideration.

The more significant consideration is a pragmatic one: State practice that escapes public attention is not available as corroboration (or rebuttal) of a customary rule. For one thing, it is difficult to ascertain the quantity or representativeness of relevant State practice. Some governments have publicly claimed that they do not engage in espionage,[15] but the veracity of such claims is hard to determine. Even when certain covert actions

14 International Law Association ("ILA"), Committee on the Formation of Customary International Law, "Statement of Principles Applicable to the Formation of General Customary International Law: Report of the Sixty-Ninth Conference" (London, 25–29 July 2000) 15. See also, e.g., Alexandra H Perina, "Black Holes and Open Secrets: The Impact of Covert Action on International Law" (2015) 53 Col J Transnatl L 507, 568.
15 See, e.g., "Peru President to Cut Short APEC Summit Visit", Associated Press (14 November 2009) (Chilean government spokesperson claiming, "Chile does not spy"); "Indonesia Recalls Ambassador after Leaked Documents Reveal Australia Spied on President Susilo Bambang Yudhoyono", ABC (18 November 2013) (Indonesian foreign minister claiming, "We don't do it").

(such as the SolarWinds hack) are the subject of leaks, the information available is invariably incomplete. It may be impossible to identify with certainty the author of a covert operation, or even to discern whether a public or private actor was responsible. Many purported "disclosures" are based on allegations unsubstantiated by persuasive evidence.[16] States accused of espionage frequently deny the allegations, commonly asserting a political motivation underpinning the charges levied against them.[17]

The clandestine character of espionage also renders difficult the necessary ascertainment of *opinio juris*. For their part, States accused of carrying out espionage frequently decline to comment on those allegations at all. For example, in 2013, British officials declined to answer questions on evidence leaked by Edward Snowden, a former contractor of the United States' National Security Agency (NSA), that its intelligence agencies had tapped the phones of European leaders, citing the government's policy of not commenting on intelligence matters.[18] Some scholars infer that States which refuse to comment on allegations that they have engaged in espionage must possess a belief that such conduct is internationally unlawful — for, if not for such a belief, they would have no reason to avoid admitting to spying on other States.[19] However, it is also plausible that States' reluctance to comment on their covert conduct is driven by motivations other than a belief in the unlawfulness of espionage. The targeted State's inability to anticipate or detect a spying operation against it is often crucial to that operation's success. Even after a mission has been completed, secrecy may be essential to ensure that the target remains unaware of the spying State's newly acquired intelligence, to avoid diplomatic blowback by the targeted State or third States, to protect informants, to escape domestic political criticism, or for a variety of other reasons.[20]

16 See, e.g., assertions by Vanuatu that Australian officials had spied in Port Vila, never admitted by the Australian government: "If we had Spies in Vanuatu, we Blundered", Sydney Morning Herald (13 May 1987) 17.
17 See, e.g., the controversy surrounding accusations that a Cambodian national had engaged in espionage in Thailand in 2011: "Cambodian 'Spy' Case Draws Official Criticism", Phnom Penh Post (13 June 2011).
18 See, e.g., "German Call for Inquiry into British Embassy 'Spying'", BBC (6 November 2013).
19 See, e.g., Wright (n 1) 17; John Kish, International Law and Espionage (edited by David Turns, Martinus Nijhoff 1995) viii; Fleck (n 3) 693.
20 See possible incentives listed in Wilson v Central Intelligence Agency, 586 F 3d 171, 197–99 (2nd Cir,

In principle, States targeted by espionage operations may be another source of *opinio juris*, but the covertness of espionage poses some difficulties in this respect as well. If an intelligence operation occurs completely without the knowledge of a targeted State, that State is deprived of an opportunity to express its legal belief in response. In these circumstances, it is plainly not viable to interpret its failure to object to espionage as acquiescence in such conduct.

For some espionage operations, there is some degree of publicity surrounding them but an individual State may not be aware of whether it has been specifically targeted or the precise extent or form of intelligence activities against it. In that scenario, on the one hand, a targeted State's failure to express a legal view on intelligence operations may imply acquiescence in such practice. On the other hand, it is arguable that a State's acceptance of conduct as lawful should not be inferred in circumstances in which it had only constructive or partial knowledge of the conduct.
A competing inference in this case is that the targeted State felt that it lacked the knowledge required to make an effective complaint, or that the State accused of espionage would dismiss any objections based on "mere rumours" as opposed to verified information.[21] For example, in 2013, Papua New Guinea was hesitant to object to potential intelligence activities by the Australian government, leaked by Snowden, without verification of the factual basis for any objection. The Papua New Guinean government stated that it refused to "run [its] foreign policy by a sensational newspaper article" in a "foreign newspaper".[22]

A further alternative scenario is where a targeted State acquires knowledge of an espionage operation against it which has not yet become generally publicly known. The State's choice to refrain from publicly protesting against that practice may, once again, be construed as acquiescence in that conduct. However, it is also possible to infer

2009).
21 I C MacGibbon, "Some Observations on the Part of Protest in International Law" (1953) 30 BYBIL 293, 294–95.
22 "China and Indonesia Pressure Australia over Spy Row", Australia Network News (2 November 2013).

that a targeted State wishes to preserve the secrecy of the operation in question for reasons other than its acceptance of the conduct as legal. Public comment may highlight the State's vulnerability to intelligence intrusions and expose weaknesses in its communications and informational systems. Moreover, public statements may undermine any counterespionage operations that rely on the spying State being unaware that its activities have been detected. Again, a targeted State's legal beliefs cannot be unambiguously inferred from its silence.

For all of these reasons, the very fact that espionage occurs clandestinely, without rendering it incapable of contributing to customary rules, makes the identification of such rules more difficult.

Secondly, even to the extent that some information about inter-State espionage is publicly known (including when covert operations such as the SolarWinds hack come to light), the evidence of State practice and *opinio juris* that is available is characterised by inconsistency, a lack of representativity and equivocality.

As to State practice, the publicly available record of intelligence activities suggests that there is not a single consistent pattern of positive or negative practice by States. It is publicly known that certain large industrialised States — such as the United States, the United Kingdom, France and Russia — have extensive intelligence programs. Certain regional heavyweights, such as Australia, Brazil, South Africa and Israel, have also had numerous of their spying operations revealed.

The fact that there is publicly available evidence of espionage perpetrated by a small number of prominent States has been sufficient for some authors to conclude that espionage *per se* is not customarily prohibited.[23] Some writers have reached this conclusion on the

23 See, e.g., Deeks (n 4) 305; Katharina Ziolkowksi, "Peacetime Cyber Espionage—New Tendencies in Public International Law" in Katharina Ziolkowksi (ed), Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy (NATO Cooperative Cyber Defence Centre of Excellence 2013) 425, 446.

premise that Western, industrialised States are "specially affected" in the sense that they "have a predominant share"[24] in carrying out espionage activity, meaning that their inconsistent State practice may be considered sufficient to negate the existence of a customary prohibition. However, given that all States are liable to be targets of espionage, it is arguably not possible to identify any subset of States which are "specially affected". Even so, whether or not these States are "specially affected", the extent of their inconsistent practice may be sufficient to negate the existence of a customary prohibition on espionage (provided it is accompanied by relevant *opinio juris* that their conduct is lawful under customary international law, considered in greater depth below).

At the same time, there is also little evidence of a consistent and representative pattern of States carrying out espionage. In some scholarship, an impression exists that, provided that there is known espionage participation by the high-profile countries mentioned above, then the practice must be positively permitted as a matter of customary international law.[25] The reality is, however, that outside of these "usual suspects", known State practice leaves the vast majority of States unaccounted for. Notwithstanding rare leaks of a lower-profile State's covert intelligence activities,[26] publicly available information suggests a highly uneven spread of espionage operations within the international community of States. Numerous States' apparent non-participation in espionage, provided it is coupled with a legal belief in the unlawfulness of such practice (considered further below), augurs against the existence of an affirmative permission to spy under customary international law.

24 H Meijers, "How is International Law Made?—The Stages of Growth of International Law and the Use of its Customary Rules" (1978) 9 NYIL 3, 7.
25 See, e.g., Spencer M Beresford, "Surveillance Aircraft and Satellites: A Problem of International Law" (1960) 27 JALC 107, 114 (claiming that espionage is not forbidden under custom because "[a]ll the great powers accept and practice espionage, as a necessary part of national defense").
26 See, e.g., allegations of espionage by Senegal ("Africa is New 'El Dorado of Espionage', Leaked Intelligence Files Reveal", Guardian (24 February 2015)) and Lithuania ("Lithuania" (2004) 50 Keesing's Record of World Events 45923).

As to *opinio juris*, States' public statements have rarely articulated clear views on the legality of covert intelligence gathering. Various legal beliefs may be inferred from those statements which are in the public domain. States which admit that they have engaged in espionage typically frame their public statements in terms of the general rectitude of their conduct,[27] or a claim that other States engage in the same conduct with equal abundance.[28] The fact that a State in this position has admitted to spying may indicate its belief that such conduct is legally permissible.[29] On the other hand, the State may admit to espionage for strategic reasons. For example, it may acknowledge its conduct believing that it was unlawful but convinced that, due to a high level of toleration of espionage by other States, the negative consequences of the admission will not be serious.

As for States targeted by espionage, their reactions are also usually equivocal, leaving doubt as to whether they consider the covert operations against them to be internationally unlawful. In many cases, a targeted State refrains from criticising the act of espionage, either abstaining from comment entirely or proffering the platitude that its good relations with the spying State remain intact.[30] One assumption which may be derived from this abstention from explicit protest is that the targeted State believes that the conduct in question is lawful — in other words, that its silence on the law amounts to acquiescence.[31] However, there may be other explanations as to why a State would refrain from protest. For example, a targeted State may do so due to

27 "Tony Abbott Refuses to Apologise for Indonesian Spying Program", Sydney Morning Herald (19 November 2013) (Australian Prime Minister claiming that Australian intelligence activities were "steps we take to protect our country" and the information gathered was used to "help our friends and allies, not harm them").

28 See, e.g., "Barack Obama Seeks to Limit EU Fallout over US Spying Claims", Guardian (2 July 2013).

29 See, e.g., Edmondson (n 7) 449.

30 See, e.g., in relation to revelations of South Korean espionage in Canberra, "Spies Caught in Canberra", Sydney Morning Herald (2 May 2013) (Australian officials citing "the long-standing practice of Australian governments not to comment on intelligence matters"); "Spy Claims won't Hurt Korea Ties: Carr", Australian (2 May 2013) (Australian foreign minister claiming that the two States' relationship "is so strong, so robust, that this will have no effect on it").

31 See Beresford (n 25) 114; Deeks (n 4) 305; Gérard Cohen-Jonathan and Robert Kovar, "L'Espionnage en Temps de Paix" (1960) 6 AFDI 239, 251–53.

its own engagement in activities of the same kind. This motivation would not necessarily imply that the State in question believes in the legality of espionage, but merely that it lacks a strategic interest in drawing attention to the illegality of the practice, especially if its objections may provoke retaliatory disclosures or politically damaging allegations of hypocrisy. Indeed, media reports suggest that the Biden administration was advised that one reason that it had limited options for responding to the SolarWinds hack is that the United States itself engages in espionage prolifically.[32]

On other occasions, a targeted State may issue a public statement condemning covert intelligence collection by another State. But the legal import of such statements often remains obscure. For example, in response to Snowden's disclosures in 2013 regarding the United States' espionage against European allies, the targeted States adopted a range of ambiguous formulae to condemn the United States' conduct, none of which expressed a clear view as to its international legality. The French Foreign Minister called the alleged activities "completely unacceptable",[33] while Luxembourg's Foreign Minister described them as "disgusting".[34] In the same vein, the Biden White House, commenting on the SolarWinds attack, has stated that steps would be taken to "hold who [United States officials] believe is responsible for this … accountable",[35] while one Senator claimed that operations such as the SolarWinds hack "cannot be tolerated".[36] It is unclear whether the belief expressed by such comments is that spying is illegal or merely unfriendly.

Third States — those not directly implicated in a particular revealed intelligence operation — do not often make public comments on the

32 "Biden Orders Sweeping Assessment of Russian Hacking, Even While Renewing Nuclear Treaty", New York Times (21 January 2021).
33 "Key US-EU Trade Pact under Threat after More NSA Spying Allegations", Guardian (30 June 2013).
34 "Berlin Accuses Washington of Cold War Tactics over Snooping", Guardian (30 June 2013).
35 "White House Says it will Hold those Responsible for SolarWinds Hack Accountable within Weeks, CNN (20 February 2021).
36 "The Cybersecurity 202: Congressional Scrutiny Heats up of Government Response to the SolarWinds Hack", Washington Post (10 February 2021).

lawfulness of the operation in question. Under one view, such silence may be taken as acquiescence in the lawfulness of the conduct.[37] It is also arguable, however, that third States' silence in response to espionage missions carried out against other States communicates no legal view, as conduct by one State may demand a response only by those other States which are actually affected by its conduct.[38] A third State may lack a detailed understanding of how the intelligence gathering took place, or whether the operation in question is emblematic of more general patterns of conduct, including intelligence activities directed against itself. It may also consider that international protocol prevents it from intervening in a dispute between other States. Such concerns were evident in Finland's reaction following the 1981 discovery of the Soviet intelligence submarine stranded in Sweden's territorial waters. A Finnish spokesperson stated that the affair was regrettable but "concerned solely Sweden and the Soviet Union".[39]

Finally, the conduct of avowedly non-spying States provides little useful by way of *opinio juris* concerning the existence of a specific prohibition or permission on espionage under customary international law. A State may indeed refrain from spying out of a belief that the practice is internationally wrongful. But it may equally not spy for other reasons, such as a lack of resources, a desire to avoid conflict with other States, or even perhaps as a matter of abstract principle.

Aside from being generally inscrutable, the legal views expressed by different States are often inconsistent with each other. Some States have expressly put forward a view that espionage is not prohibited

37 A parallel may be drawn with the ICJ's decision in the Anglo-Norwegian Fisheries case, in which it found that Norway's system of drawing baselines had enjoyed "general toleration" and therefore had become "enforceable as against all States", including third States which did not share any maritime boundaries with Norway and therefore may not have had specific occasion to object to its behaviour: Anglo-Norwegian Fisheries Case (United Kingdom v Norway) (Judgment) [1951] ICJ Rep 116, 138.

38 SS 'Lotus' (France v Turkey) (Judgment) [1927] PCIJ (ser A) No 10, 97 (Judge Altamira); Michael Akehurst, "Custom as a Source of International Law" (1974–1975) 47 BYBIL 1, 40; MacGibbon (n 21) 297–98.

39 Roma Sadurska, "Foreign Submarines in Swedish Waters: The Erosion of an International Norm" (1984) 10 YJIL 34, 51.

as a matter of customary international law. *In obiter dicta* in a case otherwise addressing individual criminal liability for espionage, the Federal Supreme Court of Germany (following reunification) found that espionage sponsored by the former East Germany was permitted by default under customary international law, stating that there is no "usage to be taken into consideration permitting, prohibiting or in any other way regulating or limiting such activity in other States under customary international law".[40] There is also a public record, however, of States expressly claiming that espionage against them or other States is not permitted as a matter of customary international law. In the 1949 case of In re Flesche, a Special Criminal Court in Amsterdam held that espionage conducted outside of wartime "constitutes an international delinquency by [the sending] State against another State for which it is answerable under international law".[41] In 1993, the government of Iraq claimed in a letter to the Secretary-General of the United Nations that American and Israeli intelligence missions against it were "incompatible with all international and moral principles, norms and laws".[42] In 2013, after Snowden's extensive revelations of electronic espionage by "Five Eyes" members, officials of various South American States claimed that the United States' practice was "unacceptable, illegitimate and contrary to … international law",[43] "violate[d] international law[,] self-determination, sovereignty",[44] amounted to "a breach of international law and … an affront of (sic) the principles that must guide the relations among [nations]",[45] and had constituted "a violation of national sovereignty and … international rules of conduct currently in place".[46] A report of the Chinese government in 2014 claimed that the United States' foreign intelligence gathering

40 Espionage Prosecution Case (1991) 2 BGs 38/91, reproduced in (1991) 94 ILR 68 (Federal Supreme Court of Germany) 74.
41 In re Flesche (1949) Annual Digest and Reports of Public International Law Cases 266, 272.
42 "Letter Dated 8 March 1993 from the Permanent Representative of Iraq to the United Nations Addressed to the Secretary-General" (10 March 1993) 2.
43 "French Condemn Surveillance by NSA", NY Times (22 October 2013) (see comments of the Mexican foreign minister).
44 "Venezuelan President Decries US Call for Denying Asylum to Data Leaker", BBC (29 June 2013).
45 "Brazilian President: US Surveillance a 'Breach of International Law'", Guardian (24 September 2013).
46 "Peruvian Foreign Affairs Committee Wants Report on US Spying", BBC (9 September 2013) (see comments of the Joint Command of Peru).

"flagrantly breached international laws".[47]

Indeed, inconsistencies can arise even in the conduct of single States — in other words, many States have conducted themselves in a way that suggests the existence of a customary rule on some occasions, but in a way that negates the existence of the same rule at other times. In the aftermath of Snowden's 2013 disclosures concerning "Five Eyes" covert intelligence gathering against Asian, European and South American States, several States which described the United States' conduct as unlawful were revealed to have engaged in activities of the same sort.[48]

The consequences of the lack of sufficient State practice and opinio juris

The ultimate question is where these methodological difficulties leave the permissibility of covert intelligence collection under customary international law.

Based on the foregoing analysis, it is not possible to conclude that there is a prohibition on espionage per se under customary international law. There is a significant record of State practice which is inconsistent with a prohibition of this character. Moreover, it is not apparent that States engaging in such practice consider themselves to be acting in violation of a prohibition. Targeted States, third States and avowedly non-spying States have also not expressed an unequivocal and consistent legal view that espionage is prohibited under custom. In light of this conclusion, the default position as a matter of customary international law (under the Lotus presumption[49]) is that States are permitted to carry out covert

47 "China Demands Halt to 'Unscrupulous' US Cyber-spying", Guardian (27 May 2014).
48 For example, a 2014 report published by the Chinese government, mentioned above, claimed that electronic eavesdropping by the United States "deserve[d] to be rejected and condemned by the whole world" as a violation of international law: "China Demands Halt to Cyber-spying" (n 47). China published the report just one week after a grand jury in the Western District of Pennsylvania indicted in absentia five Chinese government officials for economic espionage against United States companies: Department of Justice (United States), "US Charges Five Chinese Military Hackers for Cyber Espionage against US Corporations and a Labor Organization for Commercial Advantage" (19 May 2014).
49 Lotus (n 38) 19.

intelligence activities. A State may lawfully do so without establishing a permissive rule positively authorising its behaviour.

However, this conclusion is without prejudice to the applicability to the practice of espionage of prohibitive rules of international law that may forbid certain manifestations of espionage. These include treaty-based rules — such as those protecting the inviolability of diplomatic premises and communications — and those rooted in customary international law, such as the prohibition on intervention in other States' internal affairs. Where espionage of a particular character or in particular circumstances falls within a treaty-based or customary prohibition, then a State wishing to assert the lawfulness of its espionage operations cannot rely merely on the absence of a specific customary prohibition on espionage as justification of its conduct. Rather, it must be able to establish a specific, positive right to spy in those circumstances. In other words, it would need to establish that its espionage operation was lawful by virtue of an exception or qualification, when it comes to espionage, to whatever international prohibitive rule would otherwise apply.

However, the same difficulties in establishing a customary prohibition on espionage also impede efforts to establish an affirmative legal entitlement to spy capable of overriding otherwise applicable prohibitions. There is insufficient evidence of any such permissive customary rule. The practice of espionage — at least that on the public record — is concentrated in a relatively small number of prominent industrialised States. States engaging in espionage have proffered only ambiguous statements defending their conduct which fall short of articulating a positive right to spy. Some other States have condemned espionage as a violation of international law. Accordingly, based on the analysis in this paper, there is no customary "right" to spy — much less one that, as ICJ case law records is necessary, meets the high standard for proving an exception to an existing and applicable rule of custom.[50]

50 See, e.g., Lotus (n 38) 34 (Judge Loder), 60 (Judge Nyholm); Admission of a State to the United Nations (Charter, Article 4) (Advisory Opinion) [1948] ICJ Rep 57, 86 (Judge Basdevat et al).

Concluding Comments

It is easy to say that the legality of specific manifestations of espionage should be assessed in light of other rules of international law which may prohibit (or indeed permit) them. Regrettably, those "other rules" are, in many cases, subject to equally fierce debates over their scope and content. For example, there is far from a consensus over the elements of a prohibited "intervention", much less whether covert intelligence collection possesses what some see as the essential "coercive" aspect.

Perhaps the truest explanation for why there has not been any momentum towards the formulation of rules of customary international law concerning espionage qua espionage — beyond the doctrinal and empirical challenges raised above — is that States have competing interests in more or less permissive approaches to this activity. Inconsistent interests exist between different States, based on factors such as their capacity to carry out espionage and the general degree of transparency in their models of government. But even individual States can have multiple incentives which are in tension with each other. To take but recent examples, software supply chains in the United States have been profoundly affected by the SolarWinds hack, while espionage from space (in the form of satellite reconnaissance) has helped to shed light on the scale of arbitrary detention of China's Uyghur population that has led supply chains of cotton to become infected by forced labour.[51] Western democracies may recoil from the first of these covert intelligence activities but welcome the latter — and yet it is difficult to formulate rules that would forbid one while allowing the other, let alone regulate the infinite variety of other espionage activities in a way that is satisfactory to any single State or the community of States as a whole. Any such rules may well remain elusive for some time yet.

51 "China's Frontier of Fear", ABC (1 November 2018).

SolarWinds and the International Law of Peacetime Intelligence Operations

*Asaf Lubin**

* Dr. Asaf Lubin is an Associate Professor of Law at Indiana University Maurer School of Law, a Faculty Associate at the Berkman Klein Center for Internet and Society at Harvard University, a Visiting Fellow at the Information Society Project of Yale Law School, a Visiting Scholar at the Federmann Cybersecurity Center at Hebrew University of Jerusalem, a Fellow at the Center for Applied Cybersecurity Research at Indiana University, and a Visiting Fellow at the Nebraska Governance and Technology Center at the University of Nebraska.

Introduction

As President of Microsoft, Brad Smith, told the Senate Intelligence Committee on 23 February 2021, the attacker of the devastating SolarWinds hack remains the only one who "knows the entirety of what they did" even months after the hack's discovery.[1] What we do already know, however, is sufficiently alarming, as summarized by cybersecurity expert Bruce Schneier:

> *"Orion is a network management product from a company named SolarWinds, with over 300,000 customers worldwide. Sometime before March, hackers working for the Russian SVR … hacked into SolarWinds and slipped a backdoor into an Orion software update. (We don't know how, but last year the company's update server was protected by the password "solarwinds123" – something that speaks to a lack of security culture.) Users who downloaded and installed that corrupted update between March and June unwittingly gave SVR hackers access to their networks … Once inside a network, SVR hackers followed a standard playbook: establish persistent access that will remain even if the initial vulnerability is fixed; move laterally around the network by compromising additional systems and accounts; and then exfiltrate data. Not being a SolarWinds customer is no guarantee of security; this SVR operation used other initial infection vectors and techniques as well. These are sophisticated and patient hackers, and we're only just learning some of the techniques involved here."*[2]

The SolarWinds hack was what is known as "a supply-chain attack, because it targets a supplier to an organization rather than an organization

1 David E. Sanger, After Russian Cyberattack, Looking for Answers and Debating Retaliation, N.Y. TIMES (Feb. 23, 2021), https://www.nytimes.com/2021/02/23/us/politics/solarwinds-hack-senate-intelligence-russia.html.
2 Bruce Schneier, The US has suffered a massive cyberbreach. It's hard to overState how bad it is, THE GUARDIAN (Dec. 23, 2020), https://www.theguardian.com/commentisfree/2020/dec/23/cyber-attack-us-security- protocols.

itself–and can affect all of a supplier's customers."[3] As Schneier explained, this is "an increasingly common way to attack networks. Other examples of this sort of attack include fake apps in the Google Play store, and hacked replacement screens for your smartphone."[4]

According to initial estimates by the Cyber Unified Coordination Group (UCG), composed of the FBI, CISA, and ODNI with support from NSA, "of the approximately 18,000 affected public and private sector customers of Solar Winds' Orion product, a much smaller number have been compromised by follow-on activity on their systems."[5] Kevin Mandia, the CEO of FireEye, narrowed that number to 50 government agencies and private companies that were "genuinely affected."[6] Regardless of the final tally and associated economic losses, the incident demonstrates the immense risk posed by supply chain attacks. This is only heightened by recent reports claiming that SolarWinds was not the sole company vulnerable on the chain and that the hackers "used Amazon Web Services cloud hosting to disguise their intrusions as benign network traffic."[7]

Based on all publicly available information, the operation was not a "cyber-attack" as the term is broadly understood in international law and international relations, but rather an intelligence gathering operation. As such, any analysis of the legality of this operation will require a careful assessment of the rules that apply to peacetime espionage. This is a politically charged exercise that requires careful precision and delicacy in the treatment of the subject matter. I particularly urge participants of the Oxford Institute for Ethics, Law and Armed Conflict's (ELAC) Oxford Process on International Law Protections in Cyberspace (hereinafter:

3 Id.
4 Id.
5 Joint Statement by the Federal Bureau of investigations (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA) (Jan. 5, 2021), https://www.cisa.gov/news/2021/01/05/joint-Statement-federal-bureau-investigation-fbi- cybersecurity-and-infrastructure.
6 Justin Katz, 50 orgs 'genuinely impacted' by SolarWinds hack, FireEye chief says, GCN (Dec. 22, 2020), https://gcn.com/articles/2020/12/22/solarwinds-hack-impact.aspx.
7 Laura Hautala, SolarWinds not the only company used to hack targets, tech execs say at hearing, CNET (Feb. 24, 2021), https://www.cnet.com/news/solarwinds-not-the-only-company-used-to-hack-targets-tech-execs-say- at-hearing/.

the Oxford Process) to look beyond a stringently formalist and positivist review, recognizing "the poverty of this narrow, overly simplistic definition of international law."[8] In adopting a context-based, process- based, policy-based, value-based, interdisciplinary account of the normative function that intelligence plays in public world order,[9] participants will be able to "paint a more representative portrait that is at once colorful in its nuance and daunting in its complexity."[10]

Within the limits of this primer, I will canvass the major battlelines within existing scholarly debates around peacetime espionage and international law. I will then propose to Oxford Process participants to recognize the existence of a customary liberty right to spy within a broader *lex specialis* field of intelligence law. I will further claim the availability of general principles of law in building the scaffolding, alongside human rights frameworks, for constraining certain foreign intelligence efforts. While this proposed framework might seem novel to international lawyers, it is commonly championed by intelligence studies and moral philosophy scholars who have long sought to rely on "Just Intelligence Theory" to regulate intelligence at three distinct temporal stages: before (*Jus Ad*), during (*Jus In*), and after (*Jus Post*) an operation.[11] I will conclude by applying this suggested framework to intelligence operations against supply chains looking at the SolarWinds hack and two other non-cyber parallels: the fallout from operation "Rubicon" (hardware supply chain) and operation "Neptune Spear" (vaccination supply chain).

8 Janet K. Levit, Bottom-up International Lawmaking: Reflections on the New Haven School of International Law, 32 YALE J. INT'L. L. 393, 413 (2007).

9 My position is grounded in the New Haven School of thought. For the five underlying intellectual commitments of this body of thought see Harold Hongju Koh, Is There a "New" New Haven School of International Law?, 32 YALE J. INT'L. L. 559, 562-564 (2007). For a New Haven School analysis of the intelligence function see Myres S. McDougal, Harold D. Lasswell. & W. Michael Reisman, The Intelligence Function and World Public Order, 46 TEMP. L.Q. 365 (1972).

10 Levit, supra note 8, at 419.

11 for a representative yet far from exhaustive list of only book-length examples see ethics of spying: a reader for the intelligence professional (jan goldman ed., Vol. 1, 2006; Vol. 2, 2009); David perry, partly cloudy: ethics in war, espionage, covert action, and interrogation (2009); peter gill and mark phythian, intelligence in an insecure world (2nd ed., 2012); Ross w. Bellaby, the ethics of intelligence: a new framework (2014); darrell cole, just war and the ethics of espionage (2014); ethics and the future of spying: technology, national security and intelligence collection (jai galliott and warren reed eds., 2016); David omand and mark phythian, principled spying: the ethics of secret intelligence (2018).

I. The Limits of the Existing Discourse

Most international legal scholars take the view that intelligence is not per se regulated by international law.[12] Some consider it to be outside the realm of law altogether, an extra-legal construct that is "neither legal nor illegal."[13] Lacking a prohibitive rule, some have gone on to endorse a Lotus presumption of residual state freedom, one in which espionage, by either cyber or non-cyber means, is a "netherworld" and in a state of "international law free-for-all".[14]

A more nuanced group of thinkers have adopted what I have previously termed a "piecemeal approach."[15] As demonstrated in Figure 3 from Fabien Lafouasse's book, L'espionnage dans le droit international[16] (see below) this group "subdivides the world of intelligence collection into constituent state acts"[17] examining the law that governs specific methods of collection through the lens of general international legal regimes, namely territorial sovereignty, non-intervention, and diplomatic and consular law.[18] In brief, spying from outer-space or from international

12 See e.g. Tallinn manual 2.0 On the international law applicable to cyber operations 168 (michael schmitt ed., 2017).

13 See e.g. John radsan, the unresolved equation of espionage and international law, 28 mich. J. Int'l l. 595, 602 (2007); Naomi hart, espionage and international law 248-249 (dissertation, 2016) (noting that Espionage is part of a "project constructing what fleur johns terms "non-legality"... accordingly, States—and authors commentating on their conduct— have... [Relegated] espionage to a zone apparently extraneous to positive international regulation, save for the circumstances in which some other rules of international law is definitively engaged.").

14 See william c. Banks, cyber espionage and electronic surveillance: beyond the media coverage, 66 emory l.J. 513, 518. See also ashley deeks, an international legal framework for surveillance, 55(2) va. J. Int'l L. 291, 301 ("Several government officials and scholars believe that the lotus approach provides the best way to think about spying in international law. For them, the idea is simply that nothing in international law forbids States from spying on each other... Spying is therefore unregulated in international law.").

15 For more on the existing literature see asaf lubin, the liberty to spy, 61 harv. Int'l. L. J. 185, 194-206 (2020).

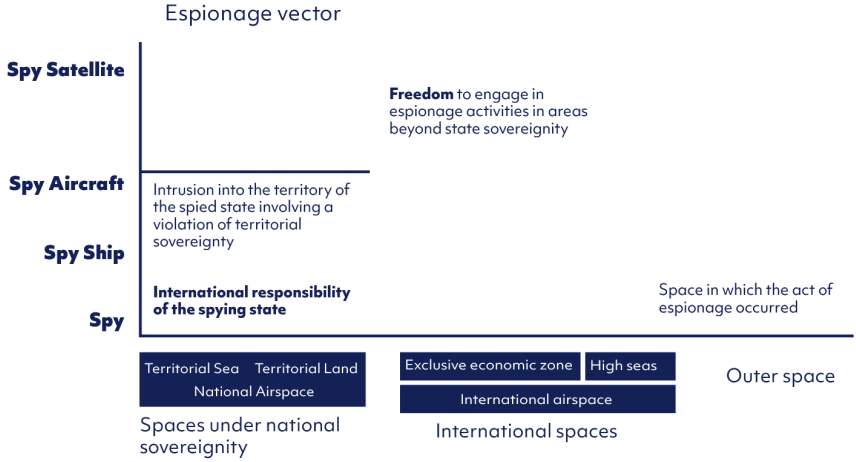
16 Fabien Lafouasse, L'espionnage dans le droit international 311 (2012) (reformatted and Translated). See similarly the concluding tables provided in craig forcese, spies without borders: international law and intelligence collection, 5 j. Nat'l sec. L. & Pol'y 179, 209 (2011) and iñaki navarrete, l'espionnage en temps de paix en droit international public, 53 canadian y.B. Int'l l. 1, 63-64 (2016).

17 Craig Forcese, Pragmatism and Principle: Intelligence Agencies and International Law, 102 Va. L. Rev. 67, 68 (2016).

18 For an excellent account that follows this approach see russel buchan, cyber espionage and International law 192-193 (2019) (suggesting the existence of a "patchwork of norms," including territorial sovereignty, diplomatic and consular law, international human rights law, and international trade law that

waters is legal whereas spying that involves territorial trespass is illegal. Spying on the office of a politician is legal whereas spying on the embassy of a diplomat is illegal. The approach is "piecemeal" in the sense that the rule-applier is called to search and identify, piece-by-piece, individual prohibitive rules (say the UN Charter principles of territorial integrity and political independence or the VCDR and VCCR rules on the inviolability of the diplomatic bag) within the vast archipelago of international law.

Figure 3. The consequences in terms of international responsibility of an act of espionage depending on the space where it occurs and depending on the vector used.



As I have argued at far greater length elsewhere, "piecemeal normative accounts fail to persuade as they ignore the open secret that all states engage in peacetime territorial and diplomatic spying;[19] they avoid an analysis of the functions of espionage and thereby the justifications for launching espionage operations;[20] they neglect to address TWAIL critiques

constrain the legality of some (if not most) political and economic cyber espionage operations).

19 If the "validity of the law presupposed a minimum efficacy of the law" as Kelsen has taught us (Hans Kelsen, Law and peace in international relations 16 (1942)) then adopting a textual myth system in complete isolation from the operational code seems like an unattainable starting point.

20 Indeed, many piecemeal scholars, as Buchan demonstrates, adopt the premise that "except in narrowly defined circumstances, political and economic cyber espionage represent a threat to the maintenance of international peace and security." (Buchan, supra note 18, at 191) This overarching Statement requires a careful review, one that I would encourage the participants in the Oxford Process to engage in.

further incentivizing a market for private surveillance by affluent states;[21] and they rest on territorial line-drawing in a surveillance age that is proving more and more unterritorial. A new normative account is thus sorely needed."[22]

II. The International Law of Intelligence (ILI) as a Lex Specialis Field of International Law

Intelligence collection, production, assessment, and verification are all parts of a professional tradecraft. Like any professional practice it has a rich history, a pool of institutions and guilds, a seemingly ever-growing list of expert terminology and acronyms, an expected set of ethical and behavioral conduct, and evolving standards, best practices, and rules of the road. We would do a massive disservice to our analysis if we completely ignored this body of special secondary rules, special institutions, special sources, and special enforcement mechanisms. A new and bold agenda for the study of espionage as a lex specialis field of international law, is one that asks us to examine the arrangements, organically devised by the international community, for settling the possible conflicts between spy and spied. The result, it is hoped, is a reimagination of this professional practice: putting into words a neglected set of unexpressed but otherwise generally accepted norms and expectations.

Such a framework, I contend, could follow the logic of the European Court of Human Rights in Zakharov v. Russia (2015) by recognizing that the regulation of secret surveillance measures may come into play

21 As I have argued, "authorizing remote spying while prohibiting territorial spying serves the goals of those States who are sufficiently powerful and technologically advanced to have the capacity to engage in such expansive forms of espionage… Third world countries are impacted twice by the piecemeal conceptualization of espionage law: once because they become the subject of these mass remote surveillance programs over which they have no control, and again because their own more primitive and less costly forms of territorial and diplomatic spying have now been deemed unlawful. What is more, a legal regime that is based on legitimizing remote forms of espionage while prohibiting territorial spying further incentivizes States to rely on corporate actors as "surveillance intermediaries" –– remote collectors and analyzers of raw digital communications and communications data." See Lubin, supra note 15, at 203-204.
22 Id., at 206.

"at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated."[23] A diagnosis of the law of peacetime intelligence operations at three distinct temporal stages follows the traditional paradigms of international law and the use of force, which themselves are grounded in the legacy of Just War Theory:

Before: *Jus Ad Explorationem* (governing the right to spy, its justifications and limitations).
During: *Jus In Exploratione* (governing the choice of means and targets in spying).
After: *Jus Post Explorationem* (governing accountability once the spying had ceased).

Adopting the Jus Ad, Jus In, Jus Post model makes for an appropriate choice, given the unique symbiosis that exists between espionage, fundamental U.N. Charter principles, and the control over international violence.

Moreover, this framework, departs from conventional wisdom by recognizing the existence of a customary liberty-right to spy shared by all sovereign nations.[24] Absent a global centralized warning and enforcement mechanism, an individual liberty to spy is a necessary pre-requisite for the functioning of our legal order. Indeed, "[t]he key to the contemporary global security system is a reliable and unremitting flow of intelligence to the pinnacle elites."[25] The notion that customary rules may emerge from what is generally treated as secret practice is of course a fraught notion.[26] The essence of the problem, argue the denouncers, is this: practice

23 See Roman Zakharov v. Russia, App. No. 47143/06, Eur. Ct. H.R., Judgment, ¶¶ 233-234 (Dec. 4, 2015).
24 For a detailed account of this customary right see Lubin, supra note 15, at 211-236.
25 25 McDougal, Lasswell. & Reisman, supra note 9, at 434.
26 See e.g. Hart, supra note 13, at 58-59 ("States' conduct in relation to espionage occurs largely in secret. That conduct which is known to the public at large does not reveal a widespread or representative pattern of practice of States either engaging in or abstaining from covert intelligence. Moreover, at least some of the relevant conduct is carried out by low-level State officials, creating uncertainty over which acts are capable of constituting evidence of the existence or absence of customary rule concerning espionage per se. When it comes to assessing States' opinio juris, it is difficult to infer States' legal beliefs from publicly known conduct, including in the form of intelligence sharing and acts surrounding treaties governing some aspects of espionage.").

must be of a public character to contribute towards the development of a custom through an iterative process of claim and counterclaim, recognition and adjustment. If peacetime espionage is conducted in the shadows and if countries are unlikely to provide statements, on the record, as to their foreign intelligence conduct and the justifications for it, then no opinio juris can be said to emerge.[27]

But as Sir Daniel Bethlehem has already argued, "one cannot make assumptions about what the law is, or reach considered conclusions on whether conduct is lawful or unlawful, until one has considered the invisible conduct, as well as the visible."[28] It is foundational in adopting a non- formalistic process-based approach, that we examine the role that shallow secrets (those secrets the general existence of which is well known and documented) play in the evolution of custom. Not only that, but it seems that with each passing generation we aggregate more and more knowledge about peacetime intelligence operations. Whistleblowing, freedom of information requests, data breaches, mandatory disclosures, increased parliamentary and executive oversight, and statutory legislation of intelligence authorities and mandates have all forced states across the world to speak out about their foreign intelligence operations in scope and magnitude like never before.[29] The silent war is no longer silent. I encourage those participants in the Oxford Process who are skeptical about the possibility of evolving customary rules around espionage to quantifiably state how much more public conduct is necessary and of

27 See generally, Iñaki Navarrete & Russel Buchan, Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions, 51 CORNELL INT'L L. J. 897 (2019) (debunking any claim of customary exceptions that would allow the functioning of intelligence law as a lex specialis field of international law). See further Robert Chesney, Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate, 5 J. NAT'L SEC. L. & POL'Y 539, 622 n. 336 (2012) (on the relationship between secrecy and expressions of lawfulness).

28 See Daniel Bethlehem, The Secret Life of International Law, 1 CAMBRIDGE J. INT'L L. & COMP. L. 23, 36 (2012) (emphasis added).

29 See e.g. Ashley Deeks, Confronting and Adapting: Intelligence Agencies and International Law, 102 VA. L. REV. 599, 615 (2016) ("[o]ne important recent development, however, is that information about intelligence activities is coming to light in near-real time, rather than decades after the fact. That means that there are greater incentives to pressure governments (through litigation, among other means) to effect immediate policy changes, because the programs at issue may be ongoing." Deeks mentions leaks (615-617), voluntary transparency (617-619), and increased physical detectability (619-621) as the three reasons for the rise in public access to information about intelligence operations).

what variety, before we can seriously consider the effects of state practice in this field.

III. Applying the New Framework to Intelligence Operations Targeting Supply Chains

Recognizing that Russia enjoys a legally enshrined liberty to spy on the United States (and that the latter enjoys a reciprocal liberty to spy on Russia) must not necessarily end with a legitimization of operations like SolarWinds. We must begin to ask deeper questions about the practice of espionage. When should uses of a sovereign nation's intelligence arm be authorized? When might we say the right to spy has been abused?[30] And what are legitimate and illegitimate means and targets for such operations, once launched?

In a series of cases involving domestic and foreign surveillance, human rights treaty bodies have laid down general requirements for the operation of intelligence, including principles of legality, necessity, proportionality, adequate safeguards, ex-ante authorization, ex-post oversight and review, transparency, and access to remedies.[31] The United States and many of its allies have already implemented such frameworks to varied degrees of success. Indeed, as noted by Ashley Deeks, "[t]he pressures on Western intelligence communities to interpret international law more strictly and apply it more robustly are only beginning."[32]

Where human rights law might be limited in its ability to restrict certain intelligence operations (say due to jurisdictional limitations, standing requirements, or challenges involving contemporary interpretation of human rights in the age of digital surveillance), general principles of law could nonetheless be utilized as either gap fillers or standard clarifiers.

30 For further discussion on the limits of the right to spy see Lubin, supra note 15, at 236-242.
31 For a useful canvassing of existing human rights jurisprudence on surveillance, further broken down in accordance with this list of requirements, see Privacy International, Guide to International Law and Surveillance (2.0) (Feb. 28, 2019), https://privacyinternational.org/long-read/993/guide-international-law-and-surveillance-20.
32 Deeks, supra note 29, at 685.

Such utilization of general principles will be specifically wise where the continued development of the law of nations is lagging behind technological developments and where existing conventions and other codification projects seem to offer little organizational help. These general principles may include the principles of rule of law, effectiveness, proportionality, good faith, fairness, and comity.

Consider the SolarWinds Hack in comparison to two other intelligence operations targeting supply chains. Operation Rubicon involved a partnership which began at the end of World War II between US and German intelligence. The operation centered around the ownership of a Swiss company, Crpyto AG, which sold radio, Ethernet, STM, GSM, phone, and fax encryption systems for generations. The two intelligence agencies "rigged the company's services so they could easily break the codes that countries used to send encrypted messages." Despite the obvious ethical challenges, "the deception and exploitation of adversaries, allies, and hundreds of unwitting Crypto employees," Bobby Ray Inman (former Director of the NSA and Deputy Director of the CIA) noted "zero qualms" in an interview, suggesting that it was "a valuable source of communications on significantly large parts of the world important to U.S. policymakers."[33]

Operation Rubicon is certainly a close call and one that merits further analysis and investigation. Nonetheless, what makes it potentially different from SolarWinds, and therefore potentially more legitimate, is that it is not indiscriminate by design. The fact that Crypto AG was able to monitor each individual sale and therefore control which targets received what compromised systems, further deciding which transmissions would be deciphered on the basis of that information, is a potential distinction of legal significance.

On the other hand, consider operation Neptune Spear to capture Osama bin Laden. In the leadup to that operation the CIA "used a sham

33 See Greg Miller, The Intelligence Coup of the Century, WASHINGTON POST (Feb. 11, 2020), https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines- espionage/.

hepatitis B vaccination project to collect DNA in the neighborhood where [Osama bin Laden] was hiding."[34] This operation was by design reckless, indiscriminate, and disproportionate with limited chances of success.[35] The operation, once discovered, caused immediate collateral damage in the form of the erosion of public trust in basic public health responses like the polio vaccine for children in Pakistan. In this regard, the failed operation, which resulted in an official CIA repudiation of the practice,[36] is closer in nature to SolarWinds. Relying on principles of necessity, efficacy, and proportionality, we may be able to conclude that one sovereign nation should not erode public trust in critical cyber emergency response tools, like commercial software updates.

Ultimately, what these examples demonstrate is that by relying on a set of general principles (as either a standalone Article 38(1)(c) source or as derived from human rights frameworks when those are applicable) we may be able to place intelligence operations targeting supply chains on a spectrum of legal and political tolerance. Such principles, which are the bedrock of the Just Intelligence Theory, could thus be used to sketch a lex specialis normative framework that is independent from the hackneyed (and likely unresolvable) debates about sovereignty and non-intervention in cyberspace.

34 See How the CIA's Fake Vaccination Campaign Endangers Us All, Scientific American. (May 1, 2013), https://www.scientificamerican.com/article/how-cia-fake-vaccination-campaign-endangers-us-all/.
35 For further reading see Saeed Shah, CIA organised fake vaccination drive to get Osama bin Laden's family DNA, The Guardian (Jul. 11, 2011), https://www.theguardian.com/world/2011/jul/11/cia-fake-vaccinations-osama- bin-ladens-dna.
36 See Letter from Lisa O. Monaco, Assistant to the President for Homeland Security and Counterterrorism (May 16, 2014), https://www.documentcloud.org/documents/1164764-monaco-letter-on-vaccine-workers.html.

Conclusion

In their 1973 seminal work, Professors McDougal, Lasswell, and Reisman provocatively concluded that the "gathering of intelligence within the territorial confines of another states is not, in and of itself, contrary to international law unless it contravenes policies of the world constitutive process affording support to protected features of internal public order."[37] Very few have ventured in their footsteps, seeking to define what those "policies" and "features" might be. I believe this is the real challenge that participants in the Oxford Process are faced with, and where we should focus most of our attention.

The legality of cyber espionage operations targeting supply chains should be analyzed on a case-by-case basis. Rule-appliers will need to consider a broad set of factual factors, including the scope, nature, purpose, and effects surrounding each operation in context and in light of the general principles of Just Intelligence Theory. A new international agenda for peacetime espionage regulation is one that seeks to constrain the most destructive elements of the trade while solidifying its core stability-enhancing functions. If the SolarWinds hack moves our discussions around the international law of intelligence in that direction, it may prove a blessing in disguise.

37 McDougal, Lasswell. & Reisman, supra note 9, at 395.

Cyber Espionage, International Law and the Protection of Digital Supply Chains

Russell Buchan *

*Dr Russell Buchan is a senior lecturer in international law at the University of Sheffield School of Law. He has published widely in the field of public international law, including two monographs: International Law and the Construction of the Liberal Peace (Hart, 2013) and Cyber Espionage and International Law (Hart, 2018).

Introduction

As more services and activities have migrated online during the Covid-19 pandemic, digital supply chains have become the lifeblood of modern society; all actors – governments, businesses and ordinary citizens – rely on their effective functioning. It therefore goes without saying that interferences with these supply chains can be hugely disruptive and even threaten the delivery of essential services.

Interferences with digital supply chains can occur at various points in the chain and take different forms. Generally speaking, malicious cyber operations can be categorised as cyber attacks or cyber network exploitation. Cyber attacks are destructive in nature insofar as they modify or delete data, compromise the functionality of computer networks or systems or, in extreme cases, produce real world physical damage. Whether cyber attacks against digital supply chains breach international law has been discussed extensively in the literature and I will not revisit those debates here. Digital supply chains are also vulnerable to acts of cyber network exploitation, that is, acts of cyber espionage that penetrate computer networks and systems in order to access and collect confidential data.

SolarWinds is a US technology company whose flagship Orion software was hacked in early 2020. The hack – 'likely Russian in origin'[1] – implanted malware in Orion and, when SolarWinds sent software updates to its customers, they unknowingly contained the malware. Upon installation, the malware created a back door into customers' computer networks and systems and enabled third parties to covertly

1 US, Joint Statement by the FBI, CISA, ODNI and NSA (2021) www.cisa.gov/news/2021/01/05/joint-Statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure.

access their confidential data. While thousands of SolarWinds customers from across the world were affected, it was largely US customers that fell victim to the hack and included government agencies, Fortune 500 businesses and individual citizens.[2]

Contrary to claims in the media and from tech companies and US politicians, the SolarWinds hack was not a cyber attack because it did not 'alter data or conduct destructive attacks'.[3] Instead, it was an act of cyber espionage. Let us assume that Russia carried out the hack. State-sponsored cyber espionage operations such as these are highly intrusive. In an international society predicated upon the principle of the sovereign equality of States,[4] the question invariably arises as to whether this type of activity is compatible with international law. This background paper explores this question. First, it provides some preliminary remarks on the interaction between international law and intelligence operations. Second, it examines whether State-sponsored cyber espionage operations against digital supply chains breach the principle of territorial sovereignty. By way of conclusion, it offers brief remarks on the international legal regulation of peacetime intelligence operations.

International Law and Espionage: Ships that Pass in the Night?

States have failed to devise international law that directly and specifically regulates peacetime intelligence operations. This has led certain international legal commentators to conclude that international law is 'remarkably oblivious'[5] to espionage and that, as a result, it is an activity that is 'neither legal nor illegal under international law'.[6] This legal assessment has been extended to cyberspace, with certain commentators arguing that cyber espionage operates in 'a legal black hole'.[7]

2 Ibid.
3 New York Times, Trump Contradicts Pompeo over Russia's Role in Hack (12 January 2021) https://www.nytimes.com/2020/12/19/us/trump-contradicts-pompeo-over-russias-role-in-hack.html.
4 Article 2(1) UN Charter 1945.
5 RA Falk, 'Foreword' in RJ Stanger (ed), Essays on Espionage and International Law (1962) v.
6 AJ Radsan, 'The Unresolved Equation of Espionage and International Law ' (2007) 28 Michigan Journal of International Law 595, 596.
7 DP Fidler, 'Tinker, Tailor, Soldier, Duqu: Why Cyberespionage is More Dangerous Than You Think' (2012)

The argument that espionage is immune to international law has never been convincing. As with many State activities, espionage is not per se regulated by international law. But as with other State activities, espionage does interact with international law. Provided of course that one is willing to look carefully enough, it is apparent that there is a plethora of principles of general international law and specialised regimes that regulate espionage insofar as they appertain to the conduct that underlies the operation.

The Principle of Territorial Sovereignty

When it comes to hacks against digital supply chains such as the one against SolarWinds, the most relevant rule of international law is the principle of territorial sovereignty. While some have suggested that it is a political principle rather than an international legal rule, State practice is converging around the latter view.[8] As a rule of international law, the principle of territorial sovereignty protects the exercise of inherently governmental functions from interference.[9] What qualifies as an inherently governmental function differs between governments depending on their political constitution. However, some functions can be only carried out by States, such as deciding who can enter and who can leave their territory.

Acts of espionage that, without consent, trespass into the physical territory of another State in order to collect confidential information breach the principle of territorial sovereignty, a conclusion that is supported by the jurisprudence of national courts[10] and the ICJ.[11] It is

5 International Journal of Critical Infrastructure Protection 28, 29.
8 MN Schmitt and L Vihul, 'Respect for Sovereignty in Cyberspace' (2017) 95 Texas Law Review 1639.
9 Island of Palmas case, 2 RIAA (Perm Ct Arb 1928) 829, 838.
10 Re Flesche, Holland, Court of Cassation (17 February 1949) International Law Reports, 272; Yao Lun v Arnold, Military Tribunal of the Supreme People's Court, China (23 November 1954) International Law Reports, 111; Gary Powers, Union of Soviet Socialist Republics, Supreme Court (19 August 1960) International Law Reports, 73-74; Re Canadian Security Intelligence Service Act [2008] FC 301, [2008] 4 FCR 230, paras 50-52.
11 Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgment (Merits) [1986] ICJ Rep 14, para 251.

for this reason that the Tallinn Manual experts agreed that an agent dispatched into the physical territory of another State in order to conduct close access cyber espionage breaches the principle of territorial sovereignty.[12]

As a matter of legal principle, territorial sovereignty applies to cyberspace but a thorny question is whether it prohibits remotely conducted cyber operations and, if so, under what circumstances. The Tallinn Manual experts agreed that sovereignty applies to cyberspace and a majority of them held that it is only those State-sponsored cyber operations that produce harm against the cyber infrastructure of another State that breach this principle. In particular, they averred that it is only those remote cyber operations that, at a minimum, compromise the functionality of a computer system or network that fall within the scope of this principle.[13] On this basis, the majority of experts determined that remotely launched cyber operations that merely intrude into the computer systems and networks of other States do not breach the principle of territorial sovereignty. Following on from this, and due to the fact that they do not affect the functionality of computer networks or systems, these experts concluded that remote access cyber espionage operations do not breach this principle.[14]

As Schmitt observes, the majority approach of the Tallinn Manual would mean that the SolarWinds hack does not violate the principle of territorial sovereignty and, in the absence of a breach of other rules of international law (e.g. diplomatic law), is lawful.[15] Recognising that this position leaves digital supply chains vulnerable to espionage, he suggests instead that, because the SolarWinds hack installed a back door in computer networks and systems and that operators had to patch this vulnerability in order to restore their integrity, it could be said that the hack caused sufficient damage to establish a breach of the principle of territorial sovereignty.

12 MN Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2017) 19.
13 Ibid 20-21.
14 Ibid 171.
15 MN Schmitt, SolarWinds Operation and International Law (21 December 202) Just Security, https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/.

This interpretation of the principle of territorial sovereignty is laudable given the need for international law to suppress malicious cyber operations such as the ones witnessed during the SolarWinds hack. But the reality is that most hacks exploit vulnerabilities in computer networks or systems and require operators to take some type of remedial action, even if the patching process is quicker and easier for one-off, opportunistic hacks than it is for more sophisticated, intensive hacks that implant permanent back doors in networks or systems. Thus, Schmitt's approach would effectively mean that any non-consensual intrusion into confidential networks or systems would breach the principle of territorial sovereignty.

Perhaps it could be said that a hack that establishes a permanent back door is more damaging than a one-off hack because it allows constant access to the network or system and the data they hold. This is not necessarily the case, however. For example, a one-off hack that exploits an easily fixable glitch in a computer network and allows access to highly sensitive data (let's say nuclear launch codes) is far more damaging that a situation where a difficult-to-fix back door is established in a network of a government department that holds innocuous data unrelated to national security.

In my view, we must divorce the principle of territorial sovereignty from the requirement of harm or damage. We now live in a Digital Age and, as the Tallinn Manual experts and the UN GGEs have concluded, States exercise sovereignty over the cyber infrastructure physically located within their territory and their sovereignty extends to the networks and systems that this infrastructure supports.[16] If this is the case, it is not clear to me why a State's inherently governmental function to decide who enters its sovereign physical territory is deserving of more protection that its decision as to who enters its sovereign cyber infrastructure. As I have previously argued, the better view is that any non-consensual intrusion into computer networks or systems that are supported by cyber

16 Tallinn Manual (n 12) Rule 1 and the UN GGE 2013 and 2015 reports.

infrastructure physically within the territory of other States amount to a breach of the principle of territorial sovereignty, regardless of whether those networks or systems are publicly or privately owned or operated.[17] This approach also finds support in State practice.[18]

Importantly, this interpretation of the principle of territorial sovereignty would prohibit remote access cyber espionage operations that penetrate without consent the computer networks and system of States, businesses and individual citizens who form part of digital supply chains. In other words, this interpretation would prohibit cyber operations such as those in witnessed in the SolarWinds hack.

Some may say that the principle of territorial sovereignty contains an 'espionage exception', that is, that through their practice and *opinio juris* States have determined that acts of espionage (and which would extend to cyber-enabled espionage) fall beyond the reach of this principle and are thus lawful.[19] States are of course entitled to carve out exceptions to rules of international law but it goes without saying that these exceptions must be clearly established in State practice and *opinio juris*, the two essential elements of customary law. In fact, as the ICJ explained in the Nicaragua case, in order to establish customary exceptions to rules a particularly strong showing of State practice and *opinio juris* is needed.[20]

State practice and *opinio juris* are difficult to identify in the context of espionage.[21] There is no doubt that espionage is widely practised within the world order. Yet, espionage is an activity that is generally committed in secret. Critically, secret State practice is methodologically irrelevant

17 Russell Buchan, Cyber Espionage and International Law (2018) Chapter 3.
18 République Française, Ministère des Armées, Droit International Appliqué aux Opérations dans le Cyberespace (2019) 7, https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+international+appliqu%C3% A9+aux+op%C3%A9rations+Cyberespace.pdf; Iran, General Staff of Iranian Armed Forces Warns of Though Reaction to Any Cyber Threat (July 2020) https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat.
19 A Deeks, 'An International Legal Framework for Surveillance' (2015) 55 Virginia Journal of International Law 291.
20 Nicaragua (n 11) para 207.
21 I Navarrete and R Buchan, 'Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions' (2019) 51 Cornell International Law Journal 897.

to the formation of customary law.[22] The reason for this is because customary law develops on the basis of claim and counterclaim between States. That said, it may be the case that the international community becomes aware of espionage via media reports, allegations by States or leaks by governmental employees. Does this constitute public State practice? For me, unless the impugned State admits involvement in espionage, leaks/allegations/reports do not amount to public State practice because, after all, the State neither endorses nor associates itself with that activity. However, allegations/reports/leaks may prompt other States to express support for espionage, which would amount to public State practice.

State practice must be coupled with *opinio juris* for custom to form, that is, the belief that such conduct is permitted by customary law. Again, this element is virtually non-existent in the context of espionage. In fact, States usually adopt a 'policy of silence' when it comes to their espionage activities, refusing to either 'confirm or deny' their involvement in such operations.[23] Very few States have justified espionage as lawful under customary law. Since the Snowden revelations, some States have been prepared to discuss their intelligence activities in the context of international law, which may pave the way for a customary espionage exception to emerge. New Zealand is a prime example in this regard. In 2020, it determined that '[t]here is a range of circumstances – in addition to pure espionage activity – in which unauthorised cyber intrusions … would not be internationally wrongful'.[24] This notwithstanding, State claims in favour of the legality of espionage are rare.

Could it be said that States have acquiesced to espionage through their failure to protest against espionage? The equation here is: silence

22 International Law Association, Committee on the Formation of Customary (General) International Law (2000) Principle 5; Prosecutor v Tadić, Case No IT-94-AR72, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 2 October 1995, para 99.
23 I Navarrete, 'L'Espionnage en Temps de Paix en Droit International Public' (2015) 53 Canadian Yearbook of International Law 1, 24.
24 New Zealand, The Application of International Law to State Activity in Cyberspace (1 December 2020) https://www.mfat.govt.nz/en/media-and-resources/ministry-Statements-and-speeches/cyber-il/.

equals acquiescence; acquiescence equals acceptance; and acceptance equals *opinio juris*. However, the silence as *opinio juris* formula must be used cautiously,[25] being employed only where States are 'in a position to react' but fail to do so.[26] As an intrinsically secret practice, States are not usually aware that espionage is being or has been committed, and this makes it difficult to attach any normative significance to their silence. More importantly, there are examples of States determining that espionage – and even cyber espionage – breaches international law. For example, while some States' reactions to the Snowden revelations were of a political character, others invoked the language of international law to condemn this activity. As an example, Mexico rejected the US's cyber espionage as 'unacceptable, illegitimate and contrary to Mexican and international law'.[27]

Given the interconnected nature of cyberspace, an important question is whether States' confidential data is protected by the principle of territorial sovereignty when it falls victim to cyber espionage while it is being stored on or transmitted through computer networks and systems supported by cyber infrastructure located within the territory of other States. First off, and on the basis of the preceding discussion, hacks against this data will breach the territorial sovereignty of the territorial State. But this does not offer much protection to the State who owns that information. One view is that the sovereignty of these States extends to such data on the basis of the principle of 'national data sovereignty', meaning that cyber espionage against this data is unlawful. Yet, there is currently little State practice to support this view.[28]

25 International Law Commission, Identification of Customary Law (2020) Conclusion 10(3); Sovereignty over Pedra Branca/Pulau Batu Puteh, Middle Rocks and South Ledge (Malaysia/Singapore), Judgment [2008] ICJ Rep 12, para 121.
26 Ibid.
27 AJ Rubin, 'French Condemn Surveillance by N.S.A', New York Times (21 October 2103). See further Buchan (n 17) Chapter 3.
28 28 Roy Schöndorf, 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations' (9 December 2020) EJIL: Talk!, https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/.

The principle of territorial sovereignty does not only protect the physicality of a State's sovereign domain from intrusion. As explained above, the essence of this principle is that it permits States to discharge inherently governmental functions without interference. If a State collects another State's confidential data while it is on foreign cyber infrastructure, and that data relates to the performance of an inherently governmental function, does it constitute unlawful interference with the exercise of that function? As things stand, the answer to this question has to be 'no'. The reason for this is because States frequently engage in espionage operations which, due to the fact that they do not involve intrusion into State territory, are not considered internationally wrongful. It is for this reason that passive 'sensing' conducted from within States is regarded as lawful.[29] Similarly, spy satellites are routinely used to conduct espionage, with most viewing this activity as compliant with international law.[30] Moreover, espionage conducted from the high seas or international airspace is not considered to breach the principle of territorial sovereignty.[31]

Conclusion

There is much hyperbole around the SolarWinds hack. The hack was an act of cyber network exploitation rather than a cyber attack and, to be fair, it was not unprecedented – its scale and sophistication is similar to cyber espionage operations carried out by other States in recent years. But international lawyers have worked themselves into a difficult position. Having previously held that cyber espionage operations fall beyond the regulatory purview of international law and are therefore lawful, they now recognise the harm caused by such acts and have sought to cast them as cyber attacks, and do so in order to reach a different conclusion as to their legality under international law.

29 Weber and Saravia v. Germany, Decision, App No 54934/00, ECtHR, 29 June 2006, para 88.
30 GA Res 41/65, Principles Relating to Remote Sensing of the Earth from Space (3 December 1986).
31 JL Cornthwaite, 'Can We Shoot Down That Drone? An Examination of International Law Issues Associated with the Use of Territorially Intrusive Aerial and Maritime Surveillance Drones in Peacetime' (2019) 52 Cornell International Law Journal 475.

As I have argued in this paper, international law regulates espionage and, in particular, it applies to the act that underlies such operations. In this way, espionage 'is less a lacuna in the legal order than it is the elephant in the room'.[32] Consequently, as any government agency, the intelligence community is subject to international law. When it comes to the protection of digital supply chains, a range of international legal rules are potentially implicated by remote access cyber espionage operations, and this paper has focused exclusively on the principle of territorial sovereignty. But other rules and regimes are apposite and should be discussed: for example, WTO law (e.g. the Paris Convention for the Protection of Industrial Property 1967) may be breached where States conduct economically motivated cyber espionage against companies, and the right to privacy under international human rights law may be infringed where natural or legal persons in a supply chain fall victim to surveillance.

To conclude, it may be the case that States recognise the utility of espionage in certain circumstances and wish to create permissive rules in favour of this activity, that is, a lex specialis of intelligence.[33] But to do so they must use existing methods of international law, for instance, by claiming these exceptions under customary law, or by embedding rules on information collection in treaties. International law cannot be founded on the basis of secret State practice and reticence.

32 S Chesterman, 'The Spy Who Came in from the Cold War: Intelligence and International Law' (2006) 27 Michigan Journal of International Law 1071, 1072.
33 A Lubin, 'The Liberty to Spy' (2020) 61 Harvard International Law Journal 185.

Dust in the (Solar)Winds: was it 'just' espionage or does international law have more to say on the protection of IT supply chains?

Antonio Coco, Talita de Souza Dias, Tsvetelina van Benthem

Introduction

The dust over the SolarWinds hack has yet to settle, more than two months after the first reports on the incident emerged. The hack, which apparently went undetected for at least nine months, exploited a vulnerability in the updates system of Orion, a network monitoring and managing software developed by Texas-based company SolarWinds and widely used by a variety of private and public actors in the United States (US) and at least seven other countries — in what has been dubbed "the largest and most sophisticated sort of operation that we have seen." Malicious code, embedded in the Orion updates, created a backdoor into the systems used among others by cybersecurity firm FireEye, Microsoft, Cisco, at least a hospital and a university, and a number of US governmental agencies, including, in particular, the Treasury, State, Commerce, and Energy Departments, as well as parts of the Pentagon. This backdoor was used to insert additional malware into affected systems, including, at the very least, spyware to exfiltrate confidential or sensitive data.

Cybersecurity firms, such as CrowdStrike, and US Federal investigators have so far linked the operation to Russia's Foreign Intelligence Service (SVR). And the official announcement that 'Black Start' — the detailed US plans to restore power in the event of a cataclysmic blackout — was compromised prompted some to speculate that the hackers were hoping to gain backdoor access into the US electric grid and laboratories developing and transporting new generations of nuclear weapons, allowing Russia to keep power from being restored in an operation similar the one it allegedly carried out in Ukraine's 2015 winter. It cannot be excluded, at this stage, that the SolarWinds hack may eventually cause detrimental effects on operational technologies. There are also reports

that yet another Orion vulnerability was used by other attackers to install malware which executes remote command code on Orion installations, i.e. to allows the attackers to remotely control the hacked systems. It is also worth noting that Orion's very purpose is to allow companies to monitor large networks connecting a number of physical devices of limited user-interfaces by implementing the so- called Simple Network Management Protocol (SNMP) protocol (see here and here). Examples of monitored devices include servers, Ethernet switches, routers, as well as the increasingly common (and pervasive) IoT devices, such as sensors, valves, power supplies (UPSs) and power distribution units.

Yet dust remains in the wind, as details about the attack are still being gradually uncovered by ongoing investigations. New information about the hack's source, method, reach and victims continue to unfold, and so will its consequences in the foreseeable future. In particular, the degree of control retained over affected systems remains unclear.

Nevertheless, it is not too early to attempt an analysis of what happened in light of international law, which, as we argued elsewhere, applies in full and by default to information and communication technologies (ICTs). Early legal (e.g. here, here and here) and policy commentary (see here and here) has looked at the incident through cyberespionage lenses, suggesting that the incident may have been 'just espionage', and thus out of the scope of international law prohibitions and protections. In particular, some have raised a tu quoque criticism against indignation from the hack: 'if Western countries do it, why can't others?'

Yet, despite this insightful narrative, the (cyber)espionage frame does not provide a full picture of the relationship between such operations and the applicable international legal framework. For whether or not cyberespionage per se is lawful under international law, the hack's method and direct or indirect consequences may have gone beyond exfiltration of state secrets to affect protected rights, persons or objects under international law. In other words, the method by which this and other cyberespionage operations

are conducted, and the harm threatened or actualised in the process, may well implicate different international rules which are worth-exploring. While searching for clear answers may be precipitated at this early stage, at the very least, it is useful to ask a range of legal questions to initiate debate. In particular, as a malicious cyber operation against key IT supply chain products used by private and public institutions, could the SolarWinds hack constitute a breach of negative and positive obligations established in international law? In this blog post (series), we raise some of those questions to get the conversation started as to whether sovereignty-as-a-rule, non-intervention, the Corfu Channel and no-harm principles, as well as certain positive and negative human rights obligations apply to this not unprecedented yet mysterious operation.

Narrowing Down Operations against the IT Supply Chain

As broad as it was, the SolarWinds hack is only one — and probably not the last — among a number of malicious cyber operations exploiting vulnerabilities in the supply chain. For instance, just a few months ago, a phishing campaign targeted providers in the Covid-19 vaccine cold supply chain, i.e. companies and institutions involved in efforts to preserve the low-temperatures in which must be kept during their storage and transportation, such as manufacturers of solar panels for storage systems. Their likely aim was to harvest credentials and intelligence for future use, including to disrupt worldwide immunisation programmers. More similarly to the SolarWinds hack, it has been alleged that a mass exfiltration of data from the African Union's IT systems, disclosed to the public in 2018, was due to a backdoor inserted in its Huawei-supplied network systems and equipment— even though evidence of such backdoor has not been found.

Whilst cybersecurity policies and measures are often focused on the protection of end-user's own systems and infrastructure, the abovementioned examples show that (weak) links in the supply chain

(especially the IT one) may be more vulnerable and thus more enticing a target for malicious actors. As aptly noted by Catriona Heinl, "[b]y *exploiting a weakness in a relatively small and weakly protected supplier, hackers can bypass even robust cybersecurity measures.*" (UNODA Commentary to GGE Norms, p. 228, § 17). What is more, compromised products or services supplied through such chain may be used by a wide variety of users, public and private, greatly facilitating the spread of malicious code and widening the pool of possible targets, as was the case in the SolarWinds hack.

One may easily understand, thus, why the United Nations Group of Governmental Experts (GGE) expressly recommended, as a norm of responsible behaviour, that *"States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products"* and *"to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions."* (GGE Report 2015, § 13(i)). Other 'voluntary, non-binding norms' identified by the GGE point in the same direction, including norm (g) on the protection of critical infrastructure and norm (j) on reporting of ICT vulnerabilities. That GGE norms are complementary to, and in some cases reflective of, international law begs the question as to the international legal framework applicable to IT supply chain attacks such as SolarWinds'.

Two preliminary considerations should frame this discussion. First, one must note that not all IT supply chains, let alone all supply chains in general, receive the same protection under international law. This depends not so much on the IT products themselves but on their purpose and use, which may or may not be covered by international law. To stay within the examples mentioned earlier in this post, SolarWinds's, Huawei's or Microsoft's products and services may be employed in the exercise of governmental functions or the provision of essential public services, including for instance those necessary to ensure the enjoyment of human rights by individuals under their jurisdiction. It is the fact that these products are used for such purposes that justifies their protection

under international law. In contrast, a number of IT products — for example those used or intended for leisure, such as videogames or streaming services — may not prima facie be covered by international legal protections.

Secondly, one must not forget that cyber operations exploiting vulnerabilities in the supply chain may take various forms. Some malicious cyber operations may be directly aimed at causing damage or harm to IT supply chain products themselves, the systems or infrastructures they cater to, or their users, by means of 'destructive' or 'disruptive' malware. Other cyber operations, à la SolarWinds, manifest themselves primarily as a breach of confidentiality of infiltrated systems, effected by means of 'spyware' or remote-control access inserted 'through the backdoor'. These may or may not cause tangible or non-tangible harm or disruption to states, companies or individuals. It is to this second type of operation that we devote our attention.

The potential infliction of such harm or disruption, in particular, prompts our analysis of two main 'families' of international obligations. On the one hand, we query whether carrying out or sponsoring a SolarWinds-type operation may constitute a breach of certain international legal duties to refrain from exploiting vulnerabilities in the IT supply chain. Such 'negative' duties may derive from a) the (supposed) rule protecting state sovereignty against unwanted intrusions; and b) the principle of non-intervention in another states' internal affairs. On the other hand, we inquire whether the SolarWinds and similar hacks implicate states' 'positive' duties to ensure the integrity of IT supply chain against threats posed by third parties, including states and non-state actors. Such duties may derive from established rules of international law like the Corfu Channel and no-harm principles, both of which require states to exercise due diligence in their use of ICTs. Finally, the violation of both negative and positive obligations to respect, protect and ensure human rights may have been implicated in the SolarWinds hack.

"The prima facie applicable international legal framework"

1. Selected duties to refrain from exploiting vulnerabilities in the IT supply chain

a. The protection of States' sovereign rights over cyber infrastructure

If the SolarWinds hack — an unauthorized intrusion, inter alia, into the US government's digital systems — was really carried out by a State actor, one may wonder whether it qualifies as a violation of the purported rule which prohibits such intrusions as violations of the victim State's territorial integrity, and thus of its sovereignty (supported, e.g. by France, the Netherlands and Iran; contra, the UK; see also Tallinn Manual 2.0, Rule 4). The difficulty with squarely fitting the SolarWinds hack into this discourse is that there is still little agreement on whether all unauthorized intrusions into a State's digital systems would constitute a violation of that rule .

As a starting point, cyber espionage seems not to be prohibited per se by international law (Tallinn Manual 2.0, Rule 32). However, such 'legality' is limited to acts of espionage itself and would not extend to damage or loss of functionality caused in the course of the data- gathering operation. In this respect, whilst a breach of territorial integrity by remote means which caused physical damage or injury (e.g. by affecting operational technology) would uncontroversially be deemed to violate the rule, the same cannot be said for operations which simply caused a 'loss of functionality'. The Tallinn Manual 2.0's Experts agreed that a cyber operation would entail a violation of the rule if it resulted in the need to repair or replace physical components of cyber infrastructure, or in *"the loss of functionality of equipment or other physical items that rely on the targeted infrastructure in order to operate"* (Tallinn Manual 2.0, at 21). In fact, such effects would be similar to physical damage. But, to date, we do not have information that the SolarWinds hack produced such result. In addition, some Experts were also of the view that a violation would occur when a cyber operation determined the need to re-install

(not merely re-boot) "*the operating system or other data upon which the targeted cyber infrastructure relies in order to perform its intended purpose*" (Tallinn Manual 2.0, at 21). Whilst the extent of the Experts' agreement on such proposition is less clear, it would not be absurd to imagine that those users who installed the infected Orion update must have had to re-install their operative systems in order to cope with the hack. As noted by Mike Schmitt, "*The best argument for a sovereignty violation on the basis of territoriality is that in order to operate the affected cyberinfrastructure with confidence, replacement of infrastructure affected by the SolarWinds operation is necessary, and it is that need that qualifies as the requisite damage.*"

In the SolarWinds case, it remains unclear whether the insertion of a software backdoor to exfiltrate data does amount to such a loss of functionality. Orion, the affected software, didn't stop working as a result of the hack — even if, to replace it or remove its backdoor, affected companies and institutions have incurred significant monetary and reputational costs. The question remains, moreover, as to whether non-physical harm that does not amount to loss of functionality, such as financial or reputational harm, could also be seen as violating the victim state's sovereignty (see Tallinn Manual 2.0, at 20-21). If not, one may also wonder if, given its scale and significance, the harm caused by the operation be nonetheless prohibited under the rule protecting sovereignty.

Equally unclear is whether the mere risk of the backdoor being used to execute commands that could have devastating physical consequences, such as the disruption of power distribution systems, would amount to a breach of affected state's sovereignty. If violations of sovereignty are deemed to arise not only from infringements upon a state's territorial integrity, but also interference with or usurpation of inherently governmental functions, a good argument can be made that obtaining remote control over key governmental IT systems might be such a violation.

b. Rule of non-intervention

That the SolarWinds hack posed a significant threat to US national security is clear. As noted above, it targeted, among many others, the US Treasury and Commerce Departments, as well as the Energy Department, the department responsible for the management of US nuclear weapons. That ensuring cyber defences appropriate to this threat will be a complex and costly endeavour is equally clear. In the American Rescue Plan announced by the Biden administration in January 2021, we read that 'in addition to the COVID-19 crisis, we also face a crisis when it comes to the nation's cybersecurity'. This recognition was coupled with a call to Congress to approve a spending of above 10 billion USD to 'remediate the SolarWinds breach and boost U.S. defenses'. It seems that the hack may have led to a quick rearrangement of priorities, and that — in times of a raging global pandemic. Could it be said, then, that such hacks may constitute acts of intervention in the internal affairs of the target state?

The elements of the customary prohibition of intervention, as set out by the International Court of Justice in Nicaragua, are the following: first, there must be an intervention 'bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely', with such matters encompassing 'the choice of a political, economic, social and cultural system, and the formulation of foreign policy' (Nicaragua, at 205); second, a wrongful intervention is one which 'uses methods of coercion in regard to such choices, which must remain free ones' (Nicaragua, at 205).

Turning to the first element, a state's reserved domain of free choice, it is not the status — private or governmental — of the targeted infrastructure that determines whether the operation falls within this domain. Rather, it is the nature of the policy choice at stake that matters. Indeed, in the SolarWinds hack, it may not be initially obvious how a state choice that must remain a free one was impacted. On reflection,

however, the breadth of the mitigation measures put forward by the Cybersecurity and Infrastructure Security Agency (CISA), together with the drastic increase in government funds dedicated to cybersecurity technology and modernisation projects could make a prima facie case for an attack that does indeed influence policy choices falling within the domaine réservé. When the threatened or actualised harm of a cyber operation results in a policy choice that the state would not have made without that operation, there may be a strong indication of an intervention impinging on an area of freedom.

The second element, coercion, forms 'the very essence of prohibited intervention' (Nicaragua, at 205). Despite its well-established existence as a core element of intervention, the contours of 'coercion', when examined closely, are highly pixelated. According to the Government of the Netherlands, 'the precise definition of coercion, and thus of unauthorised intervention, has not yet fully crystallised in international law.' In the words of the Tallinn Manual 2.0, coercion 'refers to an affirmative act designed to deprive another State of its freedom of choice, that is, to force that State to act in an involuntary manner or involuntarily refrain from acting in a particular way' (Tallinn Manual 2.0, Rule 66, at 18). In a recent blog post, Wheatley helpfully explains that coercion is about making states do things they would not otherwise do. An important question, and one with significant implications for the scope of this rule, is whether the element of coercion implies some form of intentionality vis-à-vis the result of the operation. At the Tallinn Manual process, the majority of Experts took the position that a prohibited intervention should be 'intended to influence any outcome in, or decision of, the target State' (emphasis added). A few Experts disagreed, considering that the effect of depriving the State of control over the matter in question is sufficient for it to qualify as coercive (Tallinn Manual 2.0, Rule 66, at 19). Especially in operations where the prima facie purpose is espionage, this question becomes critical. Without taking a definitive stance on the matter, it is important to note that, in the Nicaragua case, the International Court of Justice did

not speak of intention in the paragraphs specifying the content of the non- intervention rule. It only did so in the paragraphs dealing with the application of the rule to the facts, and this can be explained through the way in which the case was presented by Nicaragua: 'Nicaragua has laid much emphasis on the intentions it attributes to the Government of the United States in giving aid and support to the contras. It contends that the purpose of the policy of the United States and its actions against Nicaragua in pursuance of this policy was. from the beginning, to overthrow the Government of Nicaragua' (Nicaragua, at 240). If it is the effect that counts, then it is entirely possible for an espionage operation to be conducted through a method that breaches the principle of non-intervention. If it is the intention to coerce that matters, it would be important to clarify the ways in which such an intention could coexist with the purpose of lawful intelligence-gathering.

2. Individual protection from IT supply chain vulnerabilities: Negative and Positive Human Rights Obligations

While it has been widely reported and debated that the SolarWinds hack affected a large number of IT companies and US government departments, relatively little has been said about other victims of the operation including, in particular, state hospitals in California, Kent State University and the individuals behind these entities, including employees and customers. Even assuming that the hack was limited to a breach of data confidentiality or information- gathering, there is a possibility that private individual information was accessed by the attackers. This, in turn, raises a host of legal questions about the right to privacy under international human rights law. In particular, if personal data, such as employees' credentials, student records or patient information were accessed, to what extent would this aspect of the hack differ from electronic surveillance? And if access to such private data is akin to electronic surveillance, the question then becomes whether and to what extent the SolarWinds hack was subject to states' negative and positive

obligations to respect and protect the right to privacy under international human rights law, including human rights treaties and customary international law.

Without attempting to answer these particular questions, it is worth noting generally that, while the right to privacy is not absolute, arbitrary or unlawful violations thereof are prohibited. For instance, Article 17 of the International Covenant on Civil and Political Rights (ICCPR) permits interference with the right to privacy only where it is 'authorized by domestic law that is accessible and precise and that conforms to the requirements of the Covenant', is in pursuit of 'a legitimate aim' and 'meet[s] the tests of necessity and proportionality' (see A/69/397, para. 30, and A/HRC/41/35, para 24, and A/HRC/27/37, paras 21-30). Notably, 'any capture of communications data is potentially an interference with privacy and, further, [...] the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used. Even the mere possibility of communications information being captured creates an interference with privacy' (A/HRC/27/37, para 20).

Likewise, even assuming that the hack amounted to ('just') espionage, mere intrusions into hospital systems and databases can be damaging or at least disruptive to the provision of healthcare. This is all the more so when the biggest pandemic in the century is happening not just in the background, but on health frontlines and right in front of our eyes. In fact, even the slightest intrusion into healthcare systems can have high software or hardware repair costs, tamper with ongoing clinical research and, most importantly, interrupt the provision of critical care which, as the recent ransomware attack against Dusseldorf's University Hospital demonstrated, might well lead to patient deaths. Tellingly, Doppelpaymer, the ransomware that hit the Dusseldorf Hospital, reportedly has links to Russian groups, and was inserted through a backdoor into the hospital's system thanks to a critical vulnerability in an IT supply chain product — the Citrix application delivery controller. The

likelihood of similar scenarios deserves at least some consideration. In particular, affected states should be asking whether or not the rights to life and health have been affected or put at risk by some of the intrusions orchestrated as part of the SolarWinds hack. And it is worth bearing in mind that at least the right to life may be breached by foreseeable threats thereto, regardless of actual loss of life (see Human Rights Committee, General Comment Nº 36, paras 6-7).

That the hack also targeted a university should, furthermore, raise a red flag about a possible interference with individuals' right to education, especially considering that SolarWinds and Orion have been used as a School Network Management software by a number of higher education institution in the US.

Now, who owes these obligations, and to whom? The second question would be relatively easy to answer, once persons whose rights have been interfered with have been identified. The first question, however, raises a range of difficult (though by no means unsurmountable) additional questions. On one side, identifying the states that breached negative obligations to respect the rights to privacy, life, health and education of affected individuals requires tracing the factual origin of the attacks and legally attributing them to a duty-bearer state. While there seems to be some consensus that the hack was orchestrated by a Russian group, the exact actor and the extent of its links to the Russian government have not been officially announced. On the other side, positive human rights duties to protect the same rights are owed and may have been violated not only by the state(s) harbouring the hackers, but also by those where victims were located or which hosted IT services that were key to the enjoyment of those rights. Of course, breaches of positive human rights obligations may only have occurred to the extent that the state in question a) knew or should have known of the risk of harm arising from the cyberoperation; b) had the capacity to prevent, mitigate or redress such harm, in particular, the necessary IT infrastructure and resources; and yet, c) failed to exercise due diligence, or its best efforts to protect the rights in question.

Last but not least, States only have negative and positive obligations with respect to individuals who are within their jurisdiction. For negative obligations to protect life and privacy, at least under Articles 6 and 17 of the ICCPR, it seems that a state's extraterritorial jurisdiction may be established if it remotely conducted digital operations, to the extent that such a state exercises a) physical control over the IT/digital communications infrastructure used for the hack, b) regulatory control over third parties that physically control the relevant data (see A/HRC/27/37, paras 31-36), or c) remote control over the victims' enjoyment of human rights (see Human Rights Committee, General Comment Nº 36, para 63). Similarly, for positive human rights obligations to protect the rights to privacy and life, jurisdiction extends not only to a state's territory, but also extraterritorially to the extent of its effective control over a) persons, b) any foreseeable harm arising from its local entities, and/or c) the enjoyment of the rights in question, even if remotely (see Human Rights Committee, General Comment Nº 36, paras 21 and 63). As the UN General Assembly itself noted, 'a State may not avoid its international human rights obligations by taking action outside its territory that it would be prohibited from taking at home' (A/HRC/27/37, para 33, citing Official Records of the General Assembly, Thirty-sixth Session, annex XIX, paras. 12.2-12.3, and annex XX, para. 10.3). Digital technologies were made precisely to secure remote control over people, objects and events. So it would be a contradiction in terms, or at the very least ironical, if they could be used by a State to circumvent the jurisdictional link requirement, thereby evading international obligations.

Of note, even in case the jurisdictional requirement is satisfied, such positive human rights obligations are limited by a state's capacity to act, which means states must only do what they are reasonable capable of in the circumstances, and in accordance with their other international obligations. While states lack the power to unilaterally exercise enforcement powers extraterritorially, they can at the very least enact appropriate legislation, gather all available information about the incident,

and boost their own cybersecurity defences to prevent further harm and similar incidents in the future. It is also important to remember that not all human rights treaties contain jurisdictional clauses. For instance, the International Covenant on Economic, Social and Cultural Rights (which recognises the rights to health and education in Articles 12 and 13) does not. Thus, when it comes to human rights, tu quoque has no place: if other states are bound to respect and protect individual human rights online, so do Western democracies within and outside their borders.

3. Duties to ensure the integrity of the supply chain (selected)

Positive human rights obligations may not be the only preventive or protective duties that are implicated by the SolarWinds hack. As we have argued elsewhere, states have a patchwork of protective obligations requiring a 'due diligence' standard, among which are most prominently the Corfu Channel and the no-harm principles.

a. Corfu Channel principle

The so-called Corfu Channel principle was famously articulated by the International Court of Justice (ICJ) in the 1949 case of the same name between the UK and Albania. The principle corresponds to 'every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States' (Corfu Channel case, at 22). In other words, states have a duty to protect the rights of other states from acts that emanate from their territory or jurisdiction, regardless of attribution, i.e., who or what was responsible for the conduct. As affirmed by the Group of Experts involved in the Tallinn Manuals, the signatories of the Oxford Statements on International Law Protections in Cyberspace and a number of individual states, this duty applies by default to states' use of information and communications technologies (ICTs), given its generality and applicability across all types of state activity. That the UN GGE's voluntary, non-binding norms of

responsible state behaviour refer to this duty and different ways to fulfil it as a policy recommendation does not deprive it of its legal force.

The Corfu Channel principle is chiefly a duty of prevention which, like other due diligence obligations, depends on a state's reasonable capacity to act in the circumstances. In cyberspace as elsewhere, it requires states to prevent, stop and redress malicious operations, by digital or other means, which originate from their territory or jurisdiction, and are contrary to the rights of other states.

It appears that the SolarWinds hack originated from Russia and has had serious or at least significant adverse consequences in other states, among which the US and the UK. Thus, the key question really is whether one or more acts 'act contrary to the rights of other States' have occurred. And, here again, we might only be able to raise further questions rather than provide definitive answers. Though affecting several US institutions, it is not self-evident that the hack — in particular, the hackers' gaining of remote control over governmental systems — is actually an act contrary to the victim state's rights to sovereignty and non-intervention. Likewise, to the extent that such remote control may be used to cause serious damage in another state's territory, the key question then becomes whether the mere risk of harm is covered by the Corfu Channel principle. While it seems that the very purpose of this principle is to prevent harm and thereby address risks, this duty only arises once the origin states should have known of such a risk and it is only breached once the harm materialises (See Art. 14 Articles on the Responsibility of States for Internationally Wrongful Acts).

Moreover, it is equally unclear whether the SolarWinds hack may have been contrary to states' rights of states other than those mentioned above. There is no question that states have a duty to protect the rights of foreign states and their nationals in their own territory (see e.g., Alabama Claims Arbitration (USA v UK) (1872) 29 RIAA 125, at 127, 129, 131-132; Tehran Hostages). However, it remains controversial whether the same duty applies to aliens located outside of the duty-bearer's territory, i.e.,

either in the foreigners' own state of nationality or in another state. Most controversies surround the protection of foreign investment overseas. In fact, if the duty is read broadly, potentially any state policy that affects the economic interests or causes financial loss of overseas companies could violate international law. For instance, Saudi Arabia's decision to lower oil barrel prices by 30% caused significant economic losses to dredging companies in the US and Nigeria. Would that amount an act contrary to the rights of other states in which those companies are incorporated?

Conversely, less (but by no means non-)contentious are states' duties to protect foreign nationals from unfair competition, as found in Article 10bis of the 1967 Paris Convention for the Protection of Industrial Property which, in paragraph 2, clarifies that an act of unfair competition includes '[a]ny act of competition contrary to honest practices in industrial or commercial matters'. This provision has also been incorporated in Article 2.1 of the World Trade Organization's Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), to which both Russia and the US are notably parties. Whether or not industrial espionage is covered by those provisions, it may well be that the SolarWinds hack did constitute an act of unfair competition, given its scale, method and consequences. In particular, 18,000 institutions were affected, among which were a number of leading IT companies whose sensitive files on technologies under development may have been accessed, and whose reputation may have been permanently tainted. In this respect, States involved may have had not only a duty to refrain from it, but also a duty to prevent it by exercising due diligence.

b. The No-Harm Principle

Even if the SolarWinds hack may not have resulted in acts contrary to the rights of other states, a separate question arises as to whether the state(s) from which it originated or in whose territory or infrastructure it transited violated the so-called 'no-harm' principle. This principle requires states to

prevent, stop or redress significant transboundary harm, including when it results from lawful activity carried out by non-state actors. Two sets of questions have often been raised in this regard, especially in the context of states' use of ICTs: first, whether the no-harm principle applies beyond the environmental realm to cover 'non-ecological' harm; second, more broadly, whether the principle covers non-physical harm, such as economic losses.

The answer to the first question may be found in the International Law Commission (ILC)'s Draft articles on Prevention of Transboundary Harm from Hazardous Activities, which defines 'harm' as 'harm caused to persons, property or the environment', including 'detrimental effects on matters such as, for example, human health, industry, property, environment or agriculture'. Early ILC work had clarified that the project concerned 'all physical uses of territory giving rise to adverse physical transboundary effects' and that 'there was never an intention to propose a reduction in the scope of the topic to questions of an ecological nature'.

Finding an answer to the second question — i.e. whether the principle covers non-physical harm — may be more difficult. The ILC decided to focus only on the prevention of physical harm and 'exclude transboundary harm which may be caused by State policies in monetary, socio- economic or similar fields', admittedly 'in order to bring this topic within a manageable scope' (Draft articles on Prevention, Commentary to Article 1, para 16). Yet, this pragmatic choice was made without prejudice to the development of state practice with respect to liability for non-material harm, which was indeed well-documented in the various ILC surveys of state practice (cf. e.g. A/CN.4/543, paras 519-530). Examples of non-material injuries that have given rise to claims of liability for transboundary harm includes loss revenues or future interests arising from territorial delimitation (see A/CN.4/384, para 165), anxiety arising from potential nuclear damage (A/CN.4/543, para 520), population relocation costs (A/CN.4/471, para 259). Tellingly, in its very first survey of state practice, conducted in 1985, the ILC found that 'injury' included non-material harm, defined as "moral or qualitative harm, for example

an affront to the dignity or respect of a State, such as the broadcasting of material to another State that is in- consistent with its internal order and its territorial integrity" (A/CN.4/384, para 115). Evidence of state practice substantiating this finding, relevant for the purposes of the applicability of the no-harm principle to cyber operations, notably included: a) Article 10, paragraph 2, of the 1927 International Radiotelegraph Convention, requiring parties to operate stations in such a manner as not to interfere with the radioelectric communications of other contracting States or of persons authorized by those Government (A/CN.4/384, para 58); b) Article 35(1) of the 1932 International Telecommunication Convention, which similarly requires states parties to operate all their ICT stations, whatever their object may be, in such manner as not to interfere with the radioelectric communications or services of other parties, or of private enterprises recognised or authorised by them to conduct a radiocommunication service (A/CN.4/384, para 59); and c) Article 1 of the 1936 International Convention concerning the Use of Broadcasting in the Cause of Peace, which prohibits the broadcasting to another state of material designed to incite the population to act in a manner incompatible with the internal order and security of that state (A/CN.4/384, para 59). A similar provision requiring states to refrain from and prevent interference in other states' radio services is found in Articles 6 and 45 of the 1992 Constitution of the International Communications Union. If, since 1927, states have consistently recognised duties to prevent remote harm to or interference with other states' ICTs of the day, one would expect that the harm caused through or to the digital technologies of today is equally covered by any general duty of prevention, unless sufficient state practice and opinio juris to the contrary exists.

Finally, while questions remain as to whether or not the no-harm principle covers non- physical injury, there is little doubt that 'the required degree of care is proportional to the degree of hazard involved.' (ILC, Draft articles on Prevention, Commentary to Article 3, para 18). Therefore, the higher the foreseeable risk that vulnerabilities in the

IT supply chain (like that in SolarWinds) will be exploited to remotely control critical IT systems — such as electric and nuclear plants — the greater diligence is then required, in preventing the harmful operation, from the state in which it originated. Likewise, the higher the foreseeable risk that an IT supply chain vulnerability might affect the life and health of individuals in hospitals, the higher the diligence to be expected by the state with a view to preventing and mitigating the risk of that vulnerability's exploitation.

Conclusion

At a time in which the debate about how international law applies to ICTs is fast progressing, the SolarWinds hack has pushed such debate to the edges, bringing to the fore the issue of IT supply chain vulnerabilities and hitting on the most controversial and unsettled aspects of the relevant rules. Whether an operation à la SolarWinds hack violates a State's right to exclusive sovereign control over digital infrastructure located on its territory, whether it interferes with its internal affairs, whether it endangers an act contrary to the right of the targeted State or constitutes transboundary harm which must be prevented — all remains open to questions. Yet, these questions may be a golden opportunity for government officials and commentators alike to finally grapple with the fuzziest contours of international law applicable to ICTs and clarify the legal framework for the protection of IT supply chains.

Image credit: Arno Senoner, Unsplash

What Would Happen If States Started Looking at Cyber Operations as a 'Threat' to Use Force?

Written by Duncan B. Hollis and Tsvetelina van Benthem

First published by Lawfare on 30 March 2021

How are threats of force conveyed in cyberspace? When hackers compromised the SolarWinds Orion software in the spring of 2020, they trojanized the so-called Sunburst backdoor, a system designed to communicate with third-party providers. Through that backdoor, the hackers could execute commands, including disabling services and rebooting machines. This operation was effectively a power transfer and a significant one, at once giving those actors an "eye" into all of the victim's data and a finger on the trigger. Regardless of how one qualifies the operation against SolarWinds, how the features of such operations interact with the rules of international law requires attention. Public reporting about SolarWinds suggests the operation was limited to data exfiltration from a circumscribed group of victims that did not suggest any future use of force. Nonetheless, the case raises a question: If the presence of backdoors in a victim's network allows for future exploits capable of causing functionality losses generating destruction (or even deaths), could their presence be seen as threatening such results? More broadly, when does a cyber operation that does not itself constitute a use of force threaten force?

Article 2(4) of the U.N. Charter requires member states to refrain from both the "threat" and the "use" of force. When it comes to cyberspace, the latter prohibition has spawned seemingly endless discussions among states (for recent roundups, see, for example, here and here) and scholars alike.

International legal discourse is entering its third decade of debates on what constitutes a use of force in cyberspace, how to assess scale and effects in this new environment, and whether cyber operations that the international community has already observed, such as Stuxnet or NotPetya, qualify as a use of force or even rise to the level of an armed attack to which states can respond in self-defense. In contrast, the prohibition on the threat to use force has received almost no attention. Considering the recent drastic upsurge in cyber operations, and their diverse means, methods, and effects that individually (or collectively) imply a risk of further operations, there is a need for more dialogue about the obligation to refrain from the threat of force in cyberspace. Here, we hope to launch that conversation, exploring an otherwise underutilized obligation in the international legal arsenal that may yet have an important role to play in regulating state and state-sponsored cyber operations.

The contours of the prohibition on threats to use force are clear in its key respects. First, the state's threatened action must qualify as a use of force—threats to intervene economically or politically in another state fall outside the prohibition. Second, the threat must be to use force unlawfully. As the International Court of Justice explained in its landmark Nuclear Weapons Advisory Opinion, "The notions of 'threat' and 'use' of force under Article 2(4) of the Charter stand together in the sense that if the use of force itself in a given case is illegal—for whatever reason—the threat to use such force will likewise be illegal." Conversely, if a use of force is permissible (for example, as an exercise of self-defense), so too are threats to pursue it. Third, a threat need not be explicit (like an ultimatum)—it can also be conveyed implicitly. As noted in the Commentary to Rule 70 of the Tallinn Manual 2.0, the second edition of the most comprehensive guide on the applicability of existing international law to cyber operations, a threat can be conveyed by any means (for instance, through public pronouncements), and the substance of such threat is "to carry out cyber operations qualifying as a use of force." Explicit threats are not only the "easy" case but also the

rare one. In cyberspace, the prohibition may have much more utility for implicit cyber threats—what the Commentary to Rule 70 describes as "a cyberoperation that is used to communicate a threat to use force." In assessing the existence of an implicit threat of force, context has a major role to play. Not all manifestations of force will qualify as a threat under Article 2(4) of the U.N. Charter. All relevant contextual factors need to be considered, and the mere acquisition of weapons or demonstration of capacity (moving troops or ships) may not themselves be sufficient to constitute threats. As suggested by the Independent International Fact-Finding Mission on the Conflict in Georgia (IIFFMCG), however, if manifestations of force "are non-routine, suspiciously timed, scaled up, intensified, geographically proximate, staged in the exact mode of a potential military clash, and easily attributable to a foreign-policy message, the hostile intent is considered present and the demonstration of force manifest."

In examining threats of force, international law focuses more on an objective approach. That is, even if the existence of a signaled intention to use force lies at the core of the assessment, that assessment can be conducted by reference to objective manifestations of such intent. Importantly, a crucial element in the examination of a threat of force is its credibility. According to the IIFFMCG, it is enough for the threat to create "a calculated expectation that an unnamed challenge might incur the penalty of military force within a dispute."

The international legal community thus has a good sense of the relevant legal criteria for threats of force in the kinetic context. In the context of the conflict in Georgia, the IIFFMCG considered a number of Georgian actions, including its launching of air surveillance over the Abkhaz conflict zone in spring 2008, its participation in repeated exchanges of fire in South Ossetia, and its engagement in a comprehensive military buildup with the assistance of third parties, including acquiring modern weaponry. How might such criteria extend to cyberspace? These criteria suggest, first, that the intelligence-gathering aim of a digital operation

and the legality of espionage under international law do not preclude treating gathering of information as a factor in assessing the existence of a threat of force. Second, the acquisition of certain cyber capabilities may be relevant to the analysis. Finally, repetition of conduct matters, a point of particular relevance to cyberspace where cybersecurity experts regularly observe patterns and operational signatures.

One of the defining features of a cyber operation is its polysemous character. Technically speaking, it has always been hard to differentiate an operation that will access and leverage a vulnerability to generate confidentiality losses (like espionage) from those that can degrade or destroy the integrity or availability of data or networks (or the infrastructure the networks support). Hence, discovering a data breach today is no guarantee against a more malicious activity coming in (or already distributed) via the same means. If that malicious activity would itself clearly constitute a use of force, international lawyers must ask if the original cyber operation is itself a threat to use such force. For example, operations targeting water filtration facilities or civilian nuclear power facilities warrant careful scrutiny even if they only exhibit evidence of data breaches.

There are reasons, moreover, to think that particular features of cyber operations may warrant a threat analysis more often than in the kinetic context. The most important rationale has already been highlighted—the polysemous function of cyber operations. The same activity necessary to conduct espionage against a target is necessary to use force against it. At the same time, many cyber operations have, or at least appear to have, much larger footprints than their authors may intend; the breach of Solarwinds, for example, threatened 18,000 users, even if resulting harms were only (publicly) identified in a few hundred. Third, these operations regularly go beyond the acquisition or demonstration of a capacity to its actual deployment. That deployment, moreover, occurs within a state's networks and systems, a marked difference from troop movements or ships patrolling outside its borders. Assessing the

operation as a threat may hinge on the fact that the vehicle for force is already present within the state's territory.

Today, states and scholars repeatedly insist that international law governs state behavior in cyberspace even as they struggle (mightily, in some cases) to explain how it applies. So far, however, the discourse has focused on observable "effects" rather than threats. As a result, many (if not most) state-sponsored cyber operations labeled as espionage are treated as beyond the law's reach (international law having long ignored or exempted acts of espionage). Other debates center on which effects are regulated and how to situate them along a spectrum from armed attacks to uses of force to interventions and (for some) sovereignty violations. The approach we suggest does not attempt to displace any of these important efforts. Rather, it offers an additional regulatory perspective.

A careful consideration of the prohibition on threats to use force in cyberspace is both useful and necessary. It offers a way to reorient the law's application—to think about the law applying not just to what states do but also to what those actions threaten to do, whether expressly or implicitly. A precise threshold for assessing cyber operations through the lens of threats of force is yet to be fully fleshed out. The goal of this post is more modest—to call on states and other stakeholders to recognize the reality and thus the potential of using Article 2(4) of the U.N. Charter to bar not just uses of force in cyberspace but also threats of such force by equal measure.

The ideas of this blog post were subsequently expanded and published in Duncan B. Hollis & Tsvetelina van Benthem, 'Threatening Force in Cyberspace' in Laura Dickinson and Edward Berg (eds.), Big Data and Armed Conflict: Legal Issues Above and Below the Armed Conflict Threshold (Oxford University Press, 2022).

5 The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities

Published 2 June 2021
121 Signatories

Reiterating the commitment expressed in the First, Second and Third Oxford Statements to clarify rules of international law applicable in the use of information and communication technologies;

Considering that information operations and activities conducted by States or non-State actors through information and communications technologies have the potential to cause harm to both States and individuals, in light of their ability to reach a very wide audience instantly as exemplified by false claims surrounding COVID-19 treatments, vaccines, masks and social distancing; false or distorted claims directed at manipulating electorates or altering perceptions of climate change and technological developments; and by the incitement of violence, especially during armed conflict and periods of instability;

Understanding that the expression 'information operation[s] and activities' encompasses any coordinated or individual deployment of digital resources for cognitive purposes to change or reinforce attitudes or behaviours of the targeted audience;

Such information operations and activities include the dissemination of disinformation, misinformation, hate speech, other types of harmful speech and methods for their dissemination;

Recognizing that, as noted by the United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information, in their 2017 Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda, "disinformation and propaganda are often designed and implemented so as to mislead a population, as well as to interfere with the public's right to know and the right of individuals to seek and receive, as well as to impart, information and ideas of all kinds, regardless of frontiers,

protected under international legal guarantees of the rights to freedom of expression and to hold opinions" and that "some forms of disinformation and propaganda may harm individual reputations and privacy, or incite to violence, discrimination or hostility against identifiable groups in society";

Emphasizing that, as referenced in Principles 11 and 12 of the UN Guiding Principles on Business and Human Rights, companies have a responsibility to respect the human rights of individuals, and affirming that this responsibility extends to the impact of information operations and activities conducted using their services;

We agree that:

1. International law applies to all conduct carried out through information and communications technologies, including information operations and activities.

2. States must refrain from conducting information operations and activities when they would violate the principles of sovereignty and non-intervention in a State's internal or external affairs.

3. States must refrain from engaging in, supporting or allowing forms of speech within their jurisdiction that are prohibited under international law, such as any propaganda for war and any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence. To enforce this duty, States must prohibit by law information operations and activities amounting to such forms of speech.

4. States must refrain from engaging in, or supporting, any other information operation or activity that violates the rights of individuals within their jurisdiction, such as their right to life, health, private life, freedoms of thought and opinion, freedom of expression, including the freedom to seek, receive and impart information and ideas of all kinds, right to vote and participate in public affairs.

5. States must take measures to protect the human rights of individuals within their jurisdiction from violation by information operations or activities carried out by other States and non-state actors. Where such protective measures interfere with human rights, they must be in accordance with applicable legal requirements, such as legitimate purpose,

legality, necessity, proportionality and non-discrimination.

6. In regulating information operations and activities, States must not unduly restrict the right to freedom of expression and other rights guaranteed under international law.

7. In addressing the impact of information operations, States must ensure that information and technology companies are able to operate their services consistently with the human rights of their individual users.

8. The conduct of information operations or activities in armed conflict is subject to the applicable rules of international humanitarian law (IHL). These rules include, but are not limited to, the duty to respect and ensure respect for international humanitarian law, which entails a prohibition against encouraging violations of IHL; the duties to respect and to protect specific actors or objects, including medical personnel and facilities and humanitarian personnel and consignments; and other rules on the protection of persons who do not or no longer participate in hostilities, such as civilians and prisoners of war.

9. Conducting information operations or activities will amount to international crimes, such as genocide, including direct and public incitement thereto, war crimes and crimes against humanity, where the elements of those crimes are fulfilled.

10. The application of the aforementioned rules of international law is without prejudice to any and all other applicable rules of international law that provide protections against information operations or activities.

help
Tube

The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities

Written by Dapo Akande, Antonio Coco, Talita de Souza Dias, Duncan Hollis, James O'Brien and Tsvetelina van Benthem

First published on EJIL:Talk!, Just Security and Opinio Juris

The Internet has allowed the dissemination of content across the globe in a matter of seconds. Recommendation algorithms, found in social media platforms and search engines, have also dangerously amplified the reach of false, misleading, and violent content (see here, here, and here). Because they are geared towards engagement, the same algorithms have given rise to online 'echo chambers', whereby users are fed with the same types of viral content over and over, based on their previous clicks and assumed or stated preferences. The architecture of the Internet and the design of these algorithms have been exploited by States and non-State actors alike to sow division, spread hatred, and undermine public trust in governments and other institutions worldwide.

Recent examples abound. Violence against the Rohingya in Myanmar was spurred in large part thanks to the unrestrained and amplified dissemination of hate speech on Facebook. Foreign and domestic electoral dis- and misinformation, coupled with xenophobic discourse in the United States has polarised an already divided country, unfolding in the recent Capitol riots. And if electoral chaos, racial discrimination, and the COVID-19 pandemic weren't enough, populist leaders around the globe have spread or bolstered viral disinformation about COVID-19 and its treatment. All this activity has caused significant harm – physical and non-physical – to individuals, private entities and States.

However, existing international legal rules and principles (whether general or belonging to specific regimes) apply to information operations and activities, online and offline. That international law and the United Nations (UN) Charter, in particular, apply to ICTs has been recognised by all UN Member States, most recently through the work of the Open-ended working group on developments in the field of information and telecommunications in the context of international security (see A/AC.290/2021/CRP.2, paras 7 and 34). But the question remains as to how exactly the relevant international legal rules and principles apply in this context.

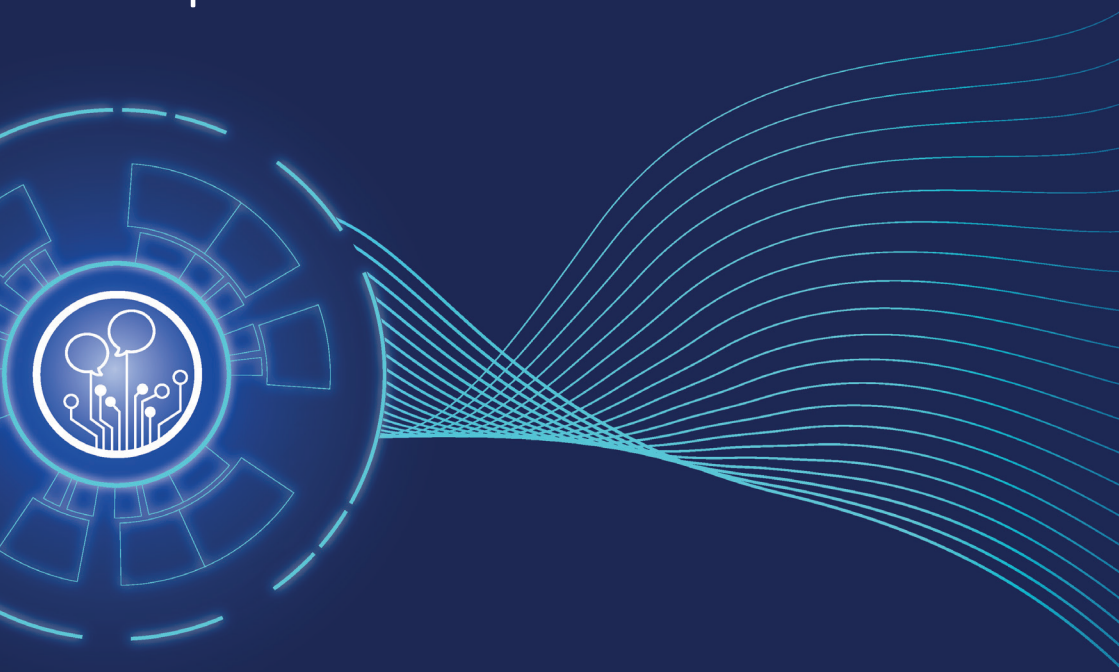
In the hope of getting some answers, the Oxford Institute for Ethics Law and Armed Conflict (ELAC) once again convened different stakeholders in the 'Oxford Process on International Law Protections in Cyberspace'. While previous Oxford Process convenings and outputs dealt with malicious cyber operations against the healthcare sector, safeguarding vaccine research and development, and foreign cyber electoral interference, this time, discussions focussed on the international regulation of 'information operations and activities'. These include disinformation, misinformation, hate speech, and other speech acts that cause physical or non-physical harm to individuals, States, and private entities – all of which are, in one way or another, governed by international law.

In the spirit of earlier iterations of the Oxford Process, participants sought to reach the widest possible degree of consensus around how international law applies to such information operations and activities. With invaluable input from participants, we produced a Statement that seeks to reflect agreement over the substance of existing international law protections, under treaty or customary international law, applying to information operations and activities. Reflecting growing consensus, the Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities refers to both positive and negative obligations of States in their foreign and domestic

behaviour pursuant to key principles and rules of international law – such as sovereignty, non-intervention, international human rights law and international humanitarian law.

We are pleased that, to date, more than 100 of the globe's most prominent international lawyers have signed onto this Fourth Oxford Statement. In doing so, we hope to continue the conversation around how international law applies to ICTs. But most importantly, we wish to see changes in behaviour by States, individuals and firms. Specifically, States and non-State actors have an international legal obligation to stop using the Internet and other ICTs to incite specific divisions, hatred, violence, and ultimately harm. We want—and need—States and companies to take responsibility to protect the information ecosystem from the most malicious and harmful uses that information operations produce.

Virtual workshop
Report



The Oxford Process on International Law Protections in Cyberspace:

The Regulation of Information Operations under International Law

13 April 2021

Executive Summary & Key Takeaways

On April 13th, 2021, the Oxford Institute for Ethics, Law and Armed Conflict (ELAC) held a virtual workshop, sponsored by Microsoft, on the regulation of information operations under international law. This workshop was part of the Oxford Process on International Law Protections in Cyberspace, an initiative seeking to identify points of consensus on international legal rules and principles in their application to specific objects of protection and methods employed by different cyber operations. This workshop was the fifth in the Oxford Process series, following on from two workshops on the protection of the healthcare sector (May and July 2020), one on the protection of electoral processes from foreign digital interference (October 2020) and one on the protection of IT supply chains (March 2021).

Information operations are both endemic and disruptive. By weaponising information, malicious actors threaten the life and health of individuals, impact privacy, political participation rights and expression, undermine trust in institutions and democratic processes, and seek to eclipse the protected zone of sovereign choice of States. From climate change through electoral processes to the management of health crises, information operations have skewed political debate and exacerbated societal divisions. At the same time, caution must be exercised in restricting speech acts, as restrictions can easily spiral into censorship and authoritarianism. Navigating this delicate balance, the fifth Oxford Process workshop sought to identify the contours of the applicable international legal rules that regulate information operations and activities. The following points emerged from the discussion:

1. International law applies to information operations and activities and is indeed a relevant and crucial framework for addressing the risks inherent in such operations.

2. In considering the threat of information operations and activities, it is important to account for both direct and short-term effects, and the long-term impact of loss of trust in institutions, democratic processes and information itself.

3. International law regulates information operations and activities through a complex system of rules that protect both State and individual interests. International human rights law, international humanitarian law and the principle of non-intervention are particularly relevant to the context of information operations.

4. International human rights law is a particularly apposite framework for evaluating information operations and activities due to its focus on human harms and the relationship between a State and individuals under its jurisdiction. States have both negative and positive duties under this regime, requiring them to refrain from behaviours that foreseeably interfere with the enjoyment of rights and to take steps to protect rights from the actions of other actors (State and non-State), respectively.

5. More work is needed to specify the content of relevant rules of international law, such as the principle of non-intervention. The element of coercion, which forms the essence of this rule, seems capable of accommodating behaviour that impacts both the ability of a State to make certain choices and its will to do so.

Background

Digitally conducted information operations have received significant attention in recent years, as we gradually become aware of the types of harm that they can generate. Just in the past year, we have seen a surge in false claims surrounding the Covid-19 vaccine, masks and social distancing, alongside digital campaigns incentivising the consumption of certain 'miraculous' supplements or products to fight the disease. In other areas, information operations containing false or distorted claims have been directed at manipulating electorates or altering perceptions of climate change and technological developments.

The aim of this workshop was to explore the international legal regulation of such operations and activities. The first session of the workshop examined the different categories of information operations, their technical characteristics and potential impact. Unpacking the types of harmful information operations is important not just for categorisation purposes, but also because these various operations may stand in a different position in relation to the rules of international law. Sessions two and three explored the content of the applicable rules of international law and sought to apply them to the identified types of information operations. Session two focused on the obligations of States vis-à-vis their own populations under international human rights law. Session three analysed information operations with a foreign element.

Summary of Sessions

Welcome and Introduction

Professors Dapo Akande (ELAC, University of Oxford) and Duncan Hollis (Temple University) gave the introductory remarks, presenting the Oxford Process to the workshop participants. Since May 2020, the Oxford Process, an initiative convened by ELAC, has sought to identify areas of consensus on the applicability of international law to operations conducted via information and communications technologies (ICTs),

focusing on specific protected objects, as well as particular means and methods through which different cyber operations have been carried out. In an attempt to move beyond the starting point that international law applies to cyberspace, the Process dives into the intricacies of particular international legal rules, specifying how these rules apply to particular instances of harmful behaviour online.

In its fifth iteration of the Oxford Process workshop series, the convenors wished to focus on information operations and activities, understood as any coordinated or individual deployment of digital resources for cognitive purposes to change or reinforce attitudes or behaviours of the targeted audience. Recent years have witnessed a proliferation of such operations and activities and demonstrated their capacity to cause harm to individual, group and State interests. Their spread, sophistication and propensity to cause harm has generated a need to investigate the content of international law as applied to the context of information operations and activities. The workshop built on the third Oxford Process event, which centred on foreign electoral interference through digital means, broadening its scope by looking beyond the electoral context while at the same time narrowing the examination to a particular method of cyber operations.

This workshop was structured into three sessions. The first session provided an overview of the current threat landscape, as well as the possible response options that could counter informational threats. Then, the second and third sessions turned to questions of law, the former looking at information operations within a State, and the latter examining the legal regulation of information operations with a foreign element.

Session 1

Information Operations: Types, Methods and Effects

Speaker: Olga Belogolova, Security Policy Lead, Influence Operations, Meta; Adjunct Assistant Professor, Center for Security Studies, Georgetown University

The presentation set the scene for the legal discussion by guiding the

participants through the threat landscape of influence operations, including the typology of observed operations, their lifecycle and effects. By outlining the perspective of a corporate actor – Meta – Ms Belogolova took the participants through the 'daily life' of these cyber operations, as well as the decision-making process that accompanies them within social media companies.

At the outset, Ms Belogolova emphasised the importance of terminology. 'Influence operations', rather than 'information operations', is the term used at Facebook, and it covers the category of broad and coordinated campaigns that are deceptive and manipulative in nature. Influence operations are thus defined as any coordinated effort to manipulate or corrupt a public debate for a strategic goal. This, then, elides the truth/falsity distinction by emphasising the component of manipulation. Importantly, the focus here is on operations that are *strategically* motivated, rather than driven by a desire for financial gain.

To identify these campaigns, teams at Facebook examine certain patterns and digital footprints. For instance, if a group of individuals is sitting in a 'troll farm' and tasked with deceiving an audience and pretending to be someone they are not, certain commonalities may become evident: the use of similar technical infrastructure, work at particular hours of the day or in shifts, sharing of the same content, dissemination in a coordinated fashion. A common thread across these operations is the lack of authenticity, as the goal is to intentionally mislead people through the use of inauthentic, fake accounts. When a group of people is financially motivated, the digital footprint of their operation may differ significantly: for instance, there may be less incentive to hide one's identity. Similarly, certain groups may coordinate their activities – political groups, for instance – while posting under their actual identities and therefore may not be engaged in malign activity. The key task, therefore, is to create a framework for recognising patterns of behaviour that are indicative of an influence operation and use this framework to separate these types of activities from others that

share one or more common elements yet differ significantly in their methods, goals and effects. Ultimately, the focus is less on the content spread through the operation and more on the way the campaign is designed and the behaviour of the operators: not *what* it seeks to deceive people to believe, but *how* the deception occurs.

Following this overview of influence operations, Ms Belogolova turned to a number of important technical and conceptual distinctions. First, she pointed to a useful framework for distinguishing between categories of operations, which focuses on **A**ctor, **B**ehaviour, or **C**ontent. For instance, when it comes to certain extremist organisations, the core interest may be in curbing content coming from a particular *actor*. In the context of hate speech, the focus is on harmful *content*. And with influence operations, Ms Belogolova emphasised the *behavioural* component. Second, she explained the difference between 'trolls' and 'bots', the latter referring to automated activity. Artificial intelligence algorithms may catch bots more easily than content distributed by humans. Humans make mistakes, have their own idiosyncratic behaviours, which makes it a lot harder to identify accounts created in bulk and in a coordinated fashion.

Turning to the lifecycle of an influence operation, Ms Belogolova explained that the inception of such an operation comes with the creation of accounts – fake personas or sometimes real persons. Then comes the development of websites and content and, following this – the pushing of content to certain communities that may be sympathetic to that content and that can, in turn, spread the content to their own circles. The final stage is that of amplification. Often, these influence campaigns co-opt legitimate authentic communities to amplify their content. One example in this regard was the hiring of freelance journalists to write for PeaceData, a website run by operators associated with the Russian Internet Research Agency.

While influence operations have always accompanied human societies, it was noted that today, such operations are becoming cheaper and easier to launch. To recognise such operations, investigators are relying on regional, including linguistic, and geopolitical expertise. Across the globe, what emerges is a complex pattern of influence operations that originate in governments, government-sponsored entities, and non-governmental entities (lobbies, media organisations). An interesting trend is that of 'influence for hire', whereby the service of influencing is offered in a way that allows state actors or individuals to distance themselves from the activities they wish to engage in. This, in turn, would pose evidential difficulties in the sphere of attribution. Ms Belogolova observed that influence operations vary in their targets: some are targeted at domestic audiences; others are projecting across national frontiers. Importantly, these inauthentic behaviours often occur on different platforms, not just on social media. Blogs, petition sites, and other websites are also utilized in influence operations, and they leverage different types of audiences that may not be present on social media.

At Meta, the efforts at curbing influence operations have focused on the building of an adversarial design into their security programming and product development. Investigators seek to identify the malicious actors and influence operations by discerning their tactics and leveraging automated systems. What is unique about the system within which this behaviour unfolds is that the terrain – the information environment – is something that companies have some control over. Vulnerabilities can be patched; the environment can be modified. For instance, if one common pattern of these operations is that actors are hiding their location, then one option to counter the threat is to make location disclosure a requirement, thus mandating transparency where malicious actors seek to operate in the dark.

In concluding, Ms Belogolova observed that, beyond the concrete facts, events and processes that these campaigns seek to mislead their audiences on, a broader concern is the impact of such operations on

societal trust in institutions and information. Malicious actors capitalise on this fear, weaponising uncertainty against democratic processes. This, according to Ms Belogolova, is a whole-of-society challenge, which requires collaboration between governments, media, internet intermediaries, tech companies and civil society.

Open discussion

In the open discussion, participants inquired into operations that combine hate speech and manipulated information, and in particular circumstances where disinformation operations groom an audience in ways that ultimately make violence likely. According to some participants, if an operation falls within the scope of content-based restrictions, the disseminated pieces of information will be removed for contravening the policies of respective online platforms. One participant further noted that certain phrases are automatically considered to satisfy the criterion of 'incitement to violence'.

Another point of discussion was the use of ranking and recommendation algorithms by social media platforms, and especially the prioritisation of viral content, such as sensationalist and emotive content, to keep users engaged with the platform. One participant noted that, given this virality, it is insufficient to moderate problematic content once it is published and disseminated. According to another participant, this risk may be mitigated through policies of de-prioritisation and demotion of content following a review by fact-checkers. Certain indicia of harmful content are thus fed into the recommendation algorithms to limit the amplification of manipulated information and hate speech.

Session II

Inside the State: Information Operations and Obligations under Human Rights Law

Marko Milanovic, Professor of Public International Law, University of Nottingham

At the start of the presentation, Professor Milanovic noted that international human rights law is the only legal framework in international law that focuses on the relationship between a State and its own people. While international humanitarian law has bearing on internal operations in the context of armed conflict, the remainder of the rules typically discussed in the context of information operations – sovereignty, non-intervention, among others – do not apply to the subject of this session, that is, operations that are purely domestic. It was further emphasised that the language of international human rights law is the only language of universal scope and ambition to regulate these questions.

Terminology was not seen as a matter that the group ought to spend too much time on: 'inauthentic coordinated behaviour' and other similar terms used by technical firms do not have a legal meaning of their own. The distinction between disinformation and misinformation should similarly attract less attention than it usually does. This is because the law – both domestic and international – does not work through binaries of culpability. Thus, the choice is not between a finding of 'direct intent to deceive' and 'innocence'. Rather, international law deals with gradations of culpability, including recklessness and negligence, which do not neatly map onto the categories of disinformation and misinformation.

According to Professor Milanovic, the key questions are the following: Who is engaging in these operations? Is it the State (State organs or other entities whose conduct is attributable to the State) or another actor?

What are the obligations at stake? To begin with, there is an obligation to respect human rights, which arises under a range of rights: freedom

of thought and opinion, freedom of expression, especially in its aspect of a right to seek and impart information. Depending on the nature of the operation, other rights may also be triggered, such as the right to vote in elections, privacy, or the right to health. The majority of such operations occur in States with authoritarian or hybrid regimes where digital information operations come as part of a much larger package of measures aimed at maintaining social control over the population. Indeed, according to Professor Milanovic, this is the case in the vast majority of countries, and the information spreading on social media platforms is of much less significance than the information spread through State-controlled press and news channels. As part of the package, one may also observe other types of operations against the free press and civil society, such as DDoS operations, or even physical attacks. All these measures may form part of a general campaign, and the information operations tactics should not be divorced from their wider context. A straightforward argument can be made that these operations entail a violation of at least one human right. Equally, even where there is no coordination and the disinformation is spread spontaneously by a State agent, the activity would still violate international human rights law. The actual delivery method should not be considered determinative for the legal qualification of a particular behaviour.

A second type of obligation is the duty to protect human rights. This is a positive duty of a State to take due diligence measures to safeguard its own population against human rights violations by third parties, whether they are non-State actors or other States. Thus, there is an obligation to regulate the platforms on which harmful information operations are taking place. States have a duty to establish adequate regulation of profit-driven actors whose primary drive is not the public interest, but the maximisation of earnings. For such types of duties, the sharp-end question for democratic States is to ensure that the regulation of online platfoms does not seep into abuse, providing a basis for autocratic States to follow their example and promulgate repressive policies.

Both types of obligations can be transplanted from the State level to the structure and internal regulatory system of corporations. The United Nations Guiding Principles on Business and Human Rights, for instance, ground a corporate social responsibility to respect human rights in the language of international human rights law. Interesting scenarios arise at the intersection of authoritarian States seeking to suppress rights and corporations acting as 'defenders' of rights against such States – one example was Facebook's takedown of hateful propaganda spread by the military in Myanmar.

David Kaye, Clinical Professor of Law, University of California, Irvine

The presentation began with a note of caution on terminology, since the phrase 'information operations' was seen as originating in military usage. A regulatory approach that borrows terms from the defence establishment may lead legislators to think overexpansively of restrictions on expression. It may similarly suggest binary conceptualisations of response options – 'restrict' or 'permit' – while the regulation of expression requires a much more nuanced approach. The framework of international human rights law provides the necessary nuance through its wide and varied range and its positive and negative obligations.

Professor Kaye focused his remarks on three specific points:
First, international human rights law provides a remarkably robust statement of freedom of expression. While the right to freedom of expression is not unlimited, the test for permissible limitations is tailored in a way that requires strong justification for interference. It is also important that international bodies, such as the Human Rights Committee and regional courts, have affirmed the foundational status of freedom of expression as a prerequisite for human development. It is through this starting point that the discussion on disinformation should be viewed. Freedom of expression is a right that, by its very definition in the International Covenant on Civil and Political Rights, applies regardless of frontiers. From a human rights perspective, the bar for restrictions of expression is, and must remain, a high one to meet.

Second, disinformation campaigns impact a variety of rights beyond freedom of expression on its limb of seeking and receiving information. The mechanics of disinformation operations often rely on significant privacy intrusions. Surveillance and data mining, which often accompany disinformation, undermine trust in public institutions and processes.

Third, the rise and spread of disinformation campaigns has brought to the fore a significant degree of regulatory confusion, with States not being of one mind as to the scope of their obligations under human rights treaties in the context of information operations. According to Professor Kaye, it is time to think creatively about addressing the underlying rot in the information system, which enables and exacerbates the virality of disinformation. It is also a time to reinforce elements of the marketplace of ideas and fortify democratic spaces. This, in turn, would require investment in media infrastructure, commitment to credible sources of information, and education. To meaningfully counter the threat of such information operations, private players must provide more insight into company governance, as their functioning continues to be opaque and distanced from meaningful public oversight.

Open Discussion

In the open discussion, the participants addressed five main questions: the effects of information operations; the factors that build a case for violations of State obligations; the hijacking of human rights language by authoritarian States; the role of social media companies; and the points of consensus on the scope of international human rights law in its application to information operations.

On the effects of information operations, participants noted the importance of considering not only short-term harms, but also the longer-term erosion of trust in institutions and information. It would be a mistake, it was noted by some, to view information operations through the lens of other cyber operations with direct and immediate effects: the harms of information operations can be felt even more acutely in the long run.

On the factors that should be taken into account when considering whether a Sate has violated its human rights obligations, some participants pointed to scale ('overwhelming messaging') and denial of access to information (the prevention of the population from having access to accurate information). Others emphasised the importance of context, the culpability of the relevant State actor, the nature of the harm that the speech act produces, and the proximity between the speech act and the harm.

On the hijacking of human rights language, a number of participants expressed concern over the hijacking of terms such as 'hate speech' by political leaders seeking to suppress expression and other freedoms. One participant emphasised the metastatic quality of restrictive laws – the adoption of one restrictive piece of legislation in one jurisdiction is often quickly taken up by others.

On the role of social media companies, it was remarked by some that, quite often, such platforms may find themselves in situations of conflict between obligations under domestic law and their social responsibilities grounded in human rights and their terms of service. In such cases, these companies have a basic choice: to yield (while maintaining a presence in the country) or to resist (including, if need be, by withdrawing from the jurisdiction). This choice is related to the cost the company is willing to incur, a cost that has both a monetary aspect and a moral and geopolitical one. Beyond these costs, it was noted that resistance to the requests of government authorities may lead to very real risks to the physical safety of employees. One participant emphasised the importance of grounding content guidelines in the language of international human rights law, as this anchoring may alter the dynamics of the conversations companies have with governments. An aspect of particular importance raised in the discussions was that of transparency: companies, according to most participants, must disclose, subject to privacy protections, the parameters of their decision-making, including by reference to requests made by government authorities.

On points of consensus, the workshop participants agreed that, in the context of information operations, States are bound by both positive and negative obligations under international human rights law owed to their own population. They further agreed that, as part of their duties to respect human rights, States must refrain from spreading false information online and offline. Beyond the right to freedom of expression, it was agreed that other rights give rise to specific State duties, including the right to health, political participation rights, and the right to privacy.

Session III

Information Operations with a Foreign Element

Sarah H. Cleveland, Louis Henkin Professor of Human and Constitutional Rights, Columbia Law School

Professor Cleveland framed her presentation regarding extraterritorial application of human rights obligations to disinformation around three scenarios: first, a scenario where the State itself spreads disinformation abroad, either through its organs or through entities whose conduct is attributable to the State; second, a scenario where non-State actors operating inside the State launch a disinformation campaign in a foreign jurisdiction; third, a scenario where non-State actors outside the State spread disinformation in a foreign jurisdiction. For each scenario, the following questions were considered relevant to the question of human rights application: Where do the acts occur? Who commits the acts? Where are the harms felt and by whom?

At the outset, Professor Cleveland addressed the question of extraterritorial application of human rights treaties. It was emphasised that the question of 'extraterritoriality' is not monolithic, and that it is ultimately a matter of interpretation of a particular human rights treaty. Some human rights instruments speak of jurisdiction only, others of territory and jurisdiction, yet others seem to draw a distinction between duties to 'respect' applicable rights universally and duties to 'ensure' applicable rights subject to territorial jurisdiction. Even the positions of States typically opposing expansive interpretations of extraterritorial

application of human rights treaties must be examined with more granularity. For instance, the United States interprets the International Covenant on Civil and Political Rights as applying only to those both within its territory and subject to its jurisdiction, while at the same time accepting a wider extraterritorial scope under other treaties, such as the Convention against Torture.

Jurisdiction, according to Professor Cleveland, has been generally interpreted by human rights bodies as involving the exercise of 'effective control'. The two traditional models of jurisdiction are the spatial model (applicable to territorial spaces) and the personal model (applicable to individuals). Developing the law on jurisdiction, some international and regional mechanisms have recognized that power or control over a person need not necessarily be confined to physical control. For many rights relevant to the discussion of information operations, such as privacy and freedom of expression, interferences can occur at a great distance. No physical control over the person is necessary; it suffices to intercept one's emails. There have been attempts to fit these scenarios in the traditional models, for instance by conceiving of control over physical infrastructure, such as a server. Another approach has emerged recently through the work of the Human Rights Committee regarding the right to life. In its 2018 General Comment No. 36, the Human Rights Committee conceived of jurisdiction as exercise of power or effective control over 'enjoyment of the right to life.' While the General Comment addresses the right to life specifically, this approach can be adapted for other rights. The most difficult questions arise at the intersection of extraterritorial jurisdiction and positive obligations. Recent opinions from the Inter-American Court of Human Rights (on transboundary harms) and the Committee on the Rights of the Child (on the rights of children held in Syrian camps) point to a broadening view of extraterritorial positive obligations.

Turning to the three scenarios, Professor Cleveland considered the first scenario – a State spreading disinformation abroad – the most

straightforward one for recognising extraterritorial jurisdiction, implicating a State's duty to respect human rights. The second scenario, involving non-State actors within the State spreading disinformation abroad, according to Professor Cleveland, reaches the outer boundaries of current jurisprudence on extraterritoriality. The Inter-American Court of Human Rights and the UN Human Rights Committee, for example, recognise the duty of States to regulate the conduct of non-State entities whose operations take place in whole or in part within their territory and in other places subject to their jurisdiction, and have direct and reasonably foreseeable impact on the rights of individuals located outside their territory. The third scenario, involving non-State actors acting outside the State, is even broader, and seems to collapse the question of capacity of a State to affirmatively protect rights of persons located abroad with the existence of a positive duty to protect those rights.

Steven Wheatley, Professor of International Law, University of Lancaster
This presentation offered a reflection on the applicability of the principle of non-intervention to foreign influence campaigns. According to Professor Wheatley, this principle is capable of covering much of the harmful conduct that States would consider undesirable in international relations. At its base, the principle of non-intervention safeguards the capacity of States to make free choices. It is limited in that it does not prohibit interferences as such, it only proscribes those interferences characterised as coercive. It is the meaning of 'coercion' that has given rise to the majority of interpretative controversies related to the rule. What, then, does coercion mean in the cyber domain?

According to Professor Wheatley, the meaning of coercion is best set out in the national position of The Netherlands, which defines coercion as compelling a State to take a course of action it would not otherwise pursue. Such compulsion can be directed at a head of State, members of parliament, or even the electorate as a whole. From Professor Wheatley's review of the meaning of compulsion in domestic and international law, the core of the term seems to be directed at a

deprivation of choice. He illustrated his argument with the following hypothetical. If one wishes to make another person stay in the room, one can do a number of things. One can, for instance, physically restrain them. One could also tell the person that they will kill them if they attempt to exit the room. Both cases leave no choice to the target. One could equally tell the person that, if they stay in the room, they will be given 500 GBP. In this case, there is still choice: they may well decide not to take the 500 GBP. Most relevant to the context of information operations is the scenario where we seek to keep the person in the room by telling them there is an active shooter situation outside. This, according to Professor Wheatley, is another example of leaving no choice to the target.

It was the opinion of Professor Wheatley that fake news and lies can be coercive. Lies can suppress voter turnout, and thus alter the outcome of an election – for instance, if the population receives messages to the effect that there is an active shooter situation in their neighbourhood, and that going out to vote will put their life in peril. Deep fakes are other forms of deceptive messaging. The principle of non-intervention can accommodate these forms of compulsion, thus extending to the use of information operations relying on lies or other forms of deceptive messaging to influence decision-making in the State. Disinformation campaigns can therefore, according to Professor Wheatley, be categorised as wrongful under the non-intervention principle when their aim is to influence the decision-making processes in another State. Information campaigns that rely on truthful information were not considered wrongful under the rule. Three reasons drove this conclusion of Professor Wheatley: first, under the existing law on propaganda, good-faith commentaries are excluded from the non-intervention principle; second, it seems impossible to coerce someone with the truth; third, it may be undesirable to view truthful information as wrongful, as this may preclude States from sending factual information to populations living under authoritarian regimes.

Tilman Rodenhäuser, Legal Adviser, International Committee of the Red Cross (speaking in a personal capacity)

This presentation centred on the limits that international humanitarian law imposes on information and psychological operations in armed conflict. At the outset, Dr Rodenhäuser clarified that information operations are not new in armed conflict and are not prohibited as such. Ruses of war that mislead the adversary can be lawfully employed – a point also acknowledged in national military manuals. However, certain information operations may give rise to concerns over the protection of the civilian population.
As a first point, Dr Rodenhäuser noted that misinformation, disinformation and hate speech can lead – and have led – to displacement, impediments to humanitarian relief efforts and physical violence. For example, it has been reported in one context that rebels useed disinformation instilling fear among civilians to displace them. Thus, the spread of information operations causes real and tangible humanitarian needs and harms.

Second, international humanitarian law imposes limits on propaganda, misinformation and disinformation. For instance, the law prohibits the encouragement of violations of the law of armed conflict. Thus, conducting information operations that would encourage attacks against civilians are clearly prohibited.

Third and finally, Dr Rodenhäuser put forward a definitional question on the notion of 'attack', asking participants to consider whether an information operation can amount to an attack, as understood under international humanitarian law. Two scenarios were considered: one where an information operation encourages the killing of civilians and another where the operation deceives civilians into harming themselves (for instance, if an information operation misleads internally displaced persons into a minefield). According to Dr Rodenhäuser, the first scenario will unlikely amount to an attack as the causation would be insufficiently direct – it would rely on the behaviour of other actors, while the second scenario may present a stronger case for qualification as an attack.

Open discussion

The open discussion sequentially addressed the areas of international law raised by the speakers in their presentations, first turning to international human rights law, then proceeding to the rule of non-intervention before concluding on the law of armed conflict.

On international human rights law, one participant noted that opposition to the extraterritorial application of human rights treaties is largely due to its packaging alongside questions of concurrent application of human rights law and international humanitarian law. Further, accepting the premise that obligations can be owed extraterritorially does not mean that States are precluded from lawfully engaging in extraterritorial conduct – rather, it means that when they do so in a way that engages human rights, they must justify their behaviour under the framework of the applicable human rights law instruments. It was noted that some States are hesitant to endorse the wider position because of concerns over their capacity to implement and enforce their obligations outside national boundaries. Most participants agreed that the direction of the extraterritoriality discussion is one of accepting a broader version of the extraterritorial application of human rights treaties.

On the rule of non-intervention, one participant queried whether a firmer grounding of the principle could be found in the lack of consent of the target State. According to Professor Wheatley, the focus ought to be on the behaviour of the outside power, and in particular whether it intervened with the intention of changing aspects of the decision-making process of the victim State. A particularly robust discussion arose on the question of who is being coerced. While one participant was hesitant to accept that operations against individuals could qualify as coercion against the State, most participants agreed that the core of the question lies in whether there is a restriction of what a State wishes to achieve – a restriction that can be accomplished by targeting individuals within the State. Another contentious question concerned the scope of coercion, and whether it is confined to lies or could cover

truths. To some, sharing truths would benefit self-determination and should not be seen as covered by the rule. To others, the sharing of truths to cause a change in a course of conduct lies at the basis of a blackmail-extortion model of coercion. One participant expressed the view that the easier cases of coercion are those that affect the ability of a State to do something, rather than its will to do so. Finally, it was agreed that a critical distinction is that between actual compulsion and affective influence, and that more work is needed on determining whether coercion entails an elimination of choice or the reduction of a State's menu of options.

On the law of armed conflict, two participants noted that even if information operations are not considered attacks, they may still qualify as military operations that trigger duties to protect civilians from the dangers arising from military operations and to exercise constant care.

One other participant opined that the qualification of information operations as military operations is still not fully settled.

List of Workshop Participants

1) Christiane Ahlborn, Legal Officer, UN Office of Legal Affairs
2) Dapo Akande, Professor of Public International Law, Co-Director, Oxford Institute for Ethics, Law & Armed Conflict (ELAC), University of Oxford
3) Leonie Arendt, Policy Consultant, UN Foundation
4) Evelyn Aswad, Herman G. Kaiser Chair in International Law, University of Oklahoma
5) Karine Bannelier-Christakis, Associate professor of International Law, Université Grenoble Alpes
6) Nayia Barmpaliou, Non-Resident Expert, Cybersecurity, European Union Institute for Security Studies
7) Olga Belogolova, Security Policy Analyst, Facebook; Adjunct Assistant Professor, Center for Security Studies, Georgetown University
8) Meredith Berger, Senior Manager, Defending Democracy, Microsoft
9) Paul Berman, Legal Director, Foreign, Commonwealth & Development Office
10) Russell Buchan, Senior Lecturer in International Law, University of Sheffield
11) Scott Charney, Vice President, Security Policy, Microsoft
12) Mary-Elisabeth Chong, State Counsel, International Affairs Division, Attorney-General's Chambers, Singapore
13) Kaja Ciglic, Senior Director, Digital Diplomacy, Microsoft
14) Sarah Cleveland, Louis Henkin Professor of Human and Constitutional Rights, Columbia Law School
15) Antonio Coco, Lecturer in Public International Law, University of Essex and Visiting Fellow at ELAC, University of Oxford
16) Gary Corn, Professor of Law and Director of Technology, Law & Security Program, American University Washington College of Law
17) Enrico Cossidente, Italian Army staff officer and military legal advisor
18) Jennifer Daskal, Deputy General Counsel, US Department of Homeland Security
19) Francois Delerue, Research Fellow in Cyberdefense and International Law, Institute of Strategic Research of the Military Academy, France
20) Talita Dias, Research Fellow, Jesus College & ELAC, University of Oxford
21) Evelyn Douek, Lecturer on Law & Doctoral Candidate, Harvard Law School
22) Kristen Eichensehr, Martha Lubin Karsh and Bruce A. Karsh Bicentennial Professor of Law, University of Virginia

23) David Fidler, Adjunct Senior Fellow for Cybersecurity & Global Health, Council on Foreign Relations
24) Naomi Hart, Barrister, Essex Court Chambers
25) Duncan B. Hollis, Laura H. Carnell Professor of Law, Temple University School of Law
26) Zhixiong Huang, Professor of International Law & Vice Dean for International relations, Executive Director, Wuhan University Institute for Cyber Governance, Wuhan University
27) Graham Ingram, Chief Information Security Officer, University of Oxford
28) Eric Jensen, Professor of Law, Brigham Young University
29) Katie Johnston, DPhil candidate in International Law, University of Oxford
30) Andraz Andy Kastelic, Lead cyber stability researcher, Security and Technology Programme, UNIDIR
31) David Kaye, Clinical Professor of Law, University of California, Irvine
32) Chimène Keitner, Alfred & Hanna Fromm Professor of International Law, UC Hastings Law
33) Lucas Kello, Associate Professor of International Relations, University of Oxford
34) Harold Hongju Koh, Senior Adviser and former Legal Adviser (2009-13), Office of the Legal Adviser, US Department of State
35) Jeffrey Kovar, Assistant Legal Adviser for Political-Military Affairs, US Department of State
36) Leonhard Kreuzer, Research Fellow, Max Planck Institute for Comparative Public Law and International Law
37) Heike Krieger, Professor of Public Law and International Law, Freie Universität Berlin
38) Joanna Kulesza, Professor of Law, University of Lodz
39) Masahiro Kurosaki, Associate Professor of International Law and Director of the Study of Law, Security and Military Operations, National Defense Academy of Japan
40) Henning Lahmann, Senior Researcher, Digital Society Institute, ESMT Berlin
41) Marja Lehto, Ambassador and Senior Legal Expert, Minister of Foreign Affairs, Finland
42) Asaf Lubin, Associate Professor of Law, Indiana University Maurer School of Law
43) Ghizala M, GCHQ
44) Kubo Mačak, Legal Adviser, ICRC; Associate Professor, University of Exeter
45) Nemanja Malisevic, Director, Digital Displomacy International Lead, Defending Democracy Program, Microsoft
46) Tomohiro Mikanagi, Deputy Director-General of the International Legal Affairs Bureau, Ministry of Foreign Affairs of Japan

47) Marko Milanovic, Professor of Public International Law, University of Nottingham
48) Tomáš Minárik, Head of International Organisations and Law Unit, National Cyber and Information Security Agency of the Czech Republic
49) Harriet Moynihan, Associate Fellow, Royal Institute of International Affairs (Chatham House)
50) Jan Neutze, Senior Director, Digital Diplomacy, Microsoft
51) Kazuho Norikura, Ministry of Foreign Affairs, Japan
52) Jim O'Brien, Vice Chair, Albright Stonebridge Group
53) Giacomo Persi Paoli, Programme Lead for Security and Technology Programme, UNIDIR
54) Patryk Pawlak, Executive Officer, European Union Institute for Security Studies
55) Tilman Rodenhäuser, Legal Adviser, ICRC
56) Przemysław Roguski, Lecturer in Law, Jagiellonian University in Kraków
57) Vera Rusinova, Professor of International Law, Higher School of Economics in Moscow
58) Barrie Sander, Assistant Professor of International Justice, Leiden University
59) Michael Schmitt, Professor of International Law, University of Reading; Francis Lieber Distinguished Scholar at the Lieber Institute of the United States Military Academy (West Point)
60) Corinna Seiberth, Lawyer, Federal Department of Foreign Affairs FDFA, Directorate of International Law, International Law Division, Switzerland
61) Hansjoerg Strohmeyer, Chief of Policy Development and Studies Branch, United Nations Office for the Coordination of Humanitarian Affairs
62) Nikhil Sud, Regulatory Affairs Specialist, Albright Stonebridge Group
63) Masaru Suzuki, First Secretary, Embassy of Japan in the United Kingdom
64) John Swords, Legal Adviser and Director of the Office of Legal Affairs at NATO Headquarters
65) Wieteke Theeuwen, Legal Officer, International Law Division, Ministry of Foreign Affairs of The Netherlands
66) Tsvetelina van Benthem, Research Officer, ELAC
67) Liis Vihul, Chief Executive Officer, Cyber Law International
68) Doug W, GCHQ
69) Marguerite Walter, Attorney-Adviser, Human Rights and Refugees, Office of the Legal Adviser, US Department of State
70) Alexander Wentker, DPhil candidate in International Law, University of Oxford
71) Stephen Wheatley, Professor of International Law, University of Lancaster
72) Robert Young, Legal Counsel, Global Affairs Canada

This background paper has been further expanded on in 'Information Operations under International Law', forthcoming in (2022) Vanderbilt Journal of Transnational Law, Vol. 55.

The Regulation of Information Operations under International Law

Tsvetelina van Benthem, Talita Dias & Duncan Hollis

In recent months, we have seen a surge of false claims surrounding the covid-19 vaccine – from disappearing needles to alleged deaths of nurses that have taken the vaccine.[1] These claims, just as those on the inefficacy of masks and social distancing, or incentivising the consumption of certain 'miraculous' supplements, can cause significant harm to the life and health of individuals. Indeed, false claims can have harmful effects in a range of areas – from manipulating the electorate during democratic processes to altering perceptions of climate change or technological developments. In this paper, we define the contours of such harmful information operations, outline the applicable international legal rules, and explore areas in need of clarification or development.

Unpacking the types of harmful information operations is important not just for definitional and categorisation purposes, but also because these various operations may stand in a different position vis-à-vis the rules of international law. Much depends on the context in which the information operation takes place: for instance, the rule on self-determination advanced by some authors may apply to information operations during elections and other democratic processes, but not in other contexts. The content itself, and in particular the author's intention, will also be key in the analysis: states are, for instance, under an obligation to prohibit advocacy of racial, national or religious hatred that constitutes incitement to discrimination, hostility or violence, and that obligation includes incitements expressed through manipulated claims. For other types of manipulated information, states may restrict speech. Underlying these legal questions are some inevitable tensions. Freedom of expression must be protected, and yet certain types of speech can cause significant harm to other rights and legitimate interests. States seek to protect their

1 See, eg, 'Covid vaccine: 'Disappearing' needles and other rumours debunked' (BBC News, 20 December 2020), available at: <https://www.bbc.co.uk/news/55364865>.

internal affairs from foreign interference, yet states have an interest in continuing to conduct certain types of influence operations. These clashes of interests translate into difficulties in determining what precisely is prohibited under international law. Likewise, they emphasise the need for a careful and granular approach to the types of operations and their regulation under specific rules of international law.

This background paper consists of three parts. **Part I** explores the 'information operation' concept. **Part II** examines the applicable rules of international law. **Part III** offers initial thoughts on areas where the law might warrant clarification, elaboration, or progressive development.

I. What are Information Operations and Why are They of Concern?

While Information Operations (IOs) have existed for centuries, they have garnered increasing attention over the last decade, as states and other stakeholders came to recognize the extent to which digital technologies facilitate their formation and execution. While there is no internationally accepted definition of IOs, for the purposes of this paper, we define them as the deployment of digital resources for cognitive purposes to change or reinforce attitudes or behaviours of the targeted audience in ways that align with the authors' interests.[2] Successful IOs do not coerce targets or wear them down; they influence, persuade or convince members of the targeted audience to adopt the goals that the IO author wishes them to adopt openly and willingly.[3]

Under this definition, it becomes apparent that IOs are a regular feature of human relations. Families and friends regularly deploy online resources to get us to adopt or change our views, social norms, or political beliefs. Companies expend significant resources on marketing

2 See Duncan Hollis, The Influence of War, The War for Influence, 32 Temple Int'l & Comp. L. J. 30 (2018). For other definitional efforts, see, e.g., Kristine Berzina and Etienne Soula, Conceptualizing Foreign Interference in Europe, Alliance for Securing Democracy 6-7 (March 18, 2020); Barrie Sander, Democracy Under the Influence: Paradigms of State Responsibility for Cyber Influence operations on Elections, 18 Chinese J Int'l L 1 (2019).

3 Herbert Lin & Jackie Kerr, On Cyber-Enabled Information/Influence Warfare and Manipulation, Working Paper, Stanford CISAC (2017).

to convince us to buy their products and services. States deploy diplomacy, speeches, and other forms of strategic communication (including "propaganda") to affect the behaviour of adversaries and foreign populations.

The risks, however, are also apparent. Given the range of potential cognitive impacts IOs can generate, it becomes easy to see how they may threaten or result in a range of significant harms, such as destabilizing electoral outcomes (e.g., the right-wing occupation of the U.S. Capital on January 6, 2021), undermining public health (e.g., an "infodemic" disrupted the "coordinated, medically sound respond that is necessary to control the spread of the [COVID-19] virus") and even inciting genocide or other atrocities (e.g., the dissemination of inaccurate and hateful rhetoric on Facebook against the Rohingya in Myanmar since 2017, and the 1994 broadcasts by Radio Télévision des Mille Collines (RTLM) radio in Rwanda which would tell Hutus: "You have missed some of the enemies. You must go back there and finish them off. The graves are not yet full!").

What, then, are the types of IOs that can lead to such harms? Three widely used categories differentiate IOs based on the authors' intentions and the verifiability of the information deployed:

(1) Misinformation – when false information is shared, but no harm is intended to arise from the sharing;
(2) Disinformation – when false information is knowingly shared to cause harm; and
(3) Malinformation – when verifiable information is shared to cause harm, often by moving information designed to stay private into the public sphere (e.g., doxing).

Other ways of categorising IOs focus on transparency – is the IO author's identity publicly known, anonymous, or affirmatively misrepresented? Misrepresented IO authors may create conditions for greater harms where audiences are more likely to be persuaded (or

react) based on the assumed identity than if the author's true identity were known to them. Anonymous IO authors may also be problematic in some cases. Yet, it is important to note a long-standing tradition protecting anonymous speech (in the United States, such speech dates back to the Framers of the US Constitution).

In sum, although IOs are a regular – and often valuable – form of human interaction, the cognitive behavioural effects they can generate create strategic opportunities for those looking to cause harm among audience members.

II. How Does International Law Apply to IOs?

This section examines the applicable international legal rules. The analysis is separated into two sub-sections: 1. information operations without a transnational element, and 2. information operations with a transnational element.

1. Information operations without a transnational element

International human rights law: negative & positive obligations

International human rights law provides a fertile ground for assessing the impact of IOs on individual rights, as well as the obligations of states to respect those rights, whether in conducting such operations or protecting individuals from IOs carried out by other actors. Some IOs will originate in state authorities who direct them against the state's own population. Examples from 2020 abound. From downplaying the transmissibility and lethality of covid-19 in the United States,[4] Brazil[5] and Nicaragua[6] to unsubstantiated allegations of election fraud,[7] claims made by State

4 'Timeline: How Trump Has Downplayed The Coronavirus Pandemic' (NPR, 2 October 2020), available at: <https://www.npr.org/sections/latest-updates-trump-covid-19-results/2020/10/02/919432383/how-trump-has-downplayed-the-coronavirus-pandemic>.
5 'How Bolsonaro downplayed Covid-19 before, and after, he contracted the virus' (The Guardian, 8 July 2020), available at: <https://www.theguardian.com/world/video/2020/jul/08/how-bolsonaro-downplayed-covid-19-before-and-after-he-contracted-the-virus-video>.
6 'Sandinista leaders fall victim to coronavirus outbreak they downplayed' (The Guardian, 8 June 2020), available at: <https://www.theguardian.com/world/2020/jun/08/nicaragua-coronavirus-sandinista-leaders-fall-victim>.
7 US Election 2020: Trump's voting fraud claims explained, BBC News, available at: <https://www.bbc.

authorities can have serious adverse consequences for the life and health of individuals, as well as for their trust in democratic institutions.

Under international human rights law, states are bound by a range of negative obligations, that is, obligations to refrain from certain actions that interfere with individual human rights.[8] IOs may implicate such obligations, including the rights to life, health, privacy, freedom to seek and impart information, vote, and the prohibition of ill-treatment.[9] For starters, the right to life prohibits arbitrary deprivation of life.[10] Deprivation of life, according to the Human Rights Committee, 'involves intentional or otherwise foreseeable and preventable life-terminating harm or injury, caused by an act or omission.'[11] That state agents may, orally or in writing, be incentivising the population to imbibe detergent as a cure instead of causing life-threatening harm by beating individuals with batons should not be a relevant distinction for the purposes of negative state obligations under said right. Information (and the conduct it may instigate or prevent) can cause as much harm as direct physical acts. The same holds true under the right to health. General Comment 14 of the Committee on Economic, Social and Cultural Rights recognises that

> violations of the obligation to respect are those state actions, policies or laws that contravene the standards set out in article 12 of the Covenant and are likely to result in bodily harm, unnecessary morbidity and preventable mortality. Examples include [...] the deliberate withholding or misrepresentation of information vital to health protection or treatment.[12]

co.uk/news/av/world-us-canada-54835475>

8 While reference will be made to specific human rights law instruments, the rights examined in the paper are also protected under customary international law.

9 For a detailed analysis of these and other rights, see de Souza Dias, Coco and van Benthem, Background Paper 'The Oxford Covid-19 Vaccine (CHADOX1 NCOV-19) Development Stages and Applicable Protective Obligations under International Law' (July 2020) and de Souza Dias and van Benthem, Background Paper 'Online Electoral Disinformation: A Human Rights Law Perspective' (October 2020).

10 International Covenant on Civil and Political Rights (ICCPR), Art. 6; African Charter of Human and Peoples' Rights (ACHPR), Art. 4; American Convention on Human Rights (ACHR), Art. 4; European Convention on Human Rights (ECHR), Art. 2 (the ECHR regulates deprivation of life through limited exceptions rather than an 'arbitrariness' standard).

11 Human Rights Committee, General Comment No. 36, CCPR/C/GC/36 (Oct. 30, 2018), para. 6.

12 Committee on Economic, Social and Cultural Rights, General Comment No. 14: The Right to the High-

The rights to life and health are of particular relevance for IOs that disseminate medical disinformation.

In the context of electoral processes, state-distributed disinformation could interfere with other rights, such as the right to freedom of thought and opinion, as well as the right to seek and impart information. These rights are protected under the International Covenant on Civil and Political Rights[13] and regional human rights instruments.[14]

It is important to bear in mind that the state is not the only domestic actor whose IOs can harm interests protected under international human rights law. Non-state actors, taking advantage of the opportunities offered by social media platforms (and in particular of the operation of content-prioritising algorithms), can mount large-scale manipulation campaigns. These can, in turn, lead to significant harm. Consider QAnon, a far-right conspiracy theory and a growing movement in the United States that reportedly sprang into existence without any foreign assistance. In relation to the coronavirus pandemic, QAnon influencers on Twitter promoted the 'Mineral Miracle Supplement', advertised as a product that can prevent covid-19 symptoms, and sold by the Texas-based Genesis II Church of Health and Healing.[15] The US Food and Drug Administration had previously issued a warning about the potentially life-threatening side effects of that supplement.[16]

Even though the source of such information operations is not the state but a private entity, the state is positively bound under international human rights law to protect the rights whose enjoyment such operations

---

est Attainable Standard of Health (Art. 12), 11 August 2000, E/C.12/2000/4, para. 50.
13 ICCPR, Art. 19.
14 ACHPR, Arts. 8-9; ACHR, Art. 13; ECHR, Art. 10.
15 Marc-André Argentino, 'QAnon conspiracy theories about the coronavirus pandemic are a public health threat' (The Conversation, 8 April 2020), available at: <https://theconversation.com/qanon-conspiracy-theories-about-the-coronavirus-pandemic-are-a-public-health-threat-135515>.
16 FDA News Release, FDA warns consumers about the dangerous and potentially life threatening side effects of Miracle Mineral Solution, 12 August 2019, available at: <https://www.fda.gov/news-events/press-announcements/fda-warns-consumers-about-dangerous-and-potentially-life-threatening-side-effects-miracle-mineral>.

may imperil. According to the Human Rights Committee, 'the duty to protect life also implies that states parties should take appropriate measures to address the general conditions in society that may give rise to direct threats to life or prevent individuals from enjoying their right to life with dignity.'[17] Similarly, under the right to health, states must 'take all necessary measures to safeguard persons within their jurisdiction from infringements of the right to health by third parties.'[18] While there is no prescriptive list of positive actions required, and they vary significantly according to each right and the particular context of application, states are under an obligation to take necessary and feasible measures to prevent, mitigate, and redress harm originating from IOs that foreseeably impact the enjoyment of human rights.

The relationship between IOs and states' positive international legal obligations is complex. This is because the false or manipulated nature of the information is not the only defining characteristic of these operations. Different conceptual frames apply depending on the disseminated content and the ensuing regulatory discretion left to the state:

(a) IOs that must be prohibited by states. International human rights law prohibits certain categories of speech and obligates states to enact domestic prohibitions.[19] For instance, under art. 20 of the International Covenant on Civil and Political Rights (ICCPR),

> 1. Any propaganda for war shall be prohibited by law.
> 2. Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.

17 General Comment 36 on the right to life, para. 26. Human Rights Committee, General Comment No.6, para. 5. One aspect of these 'general conditions' is the 'prevalence of life-threatening diseases'. In its previous general comment on the right to life, the Committee noted that 'the right to life has been too often narrowly interpreted. The expression "inherent right to life" cannot properly be understood in a restrictive manner, and the protection of this right requires that States adopt positive measures. In this connection, the Committee considers that it would be desirable for States parties to take all possible measures to [...] adopt measures to eliminate [...] epidemics.'

18 CESR, General Comment 14, para. 51.

19 Prohibition is not, however, tantamount to criminalisation, and criminalisation should be reserved for the most serious of crimes - UNGA Res A/74/486, para. 8.

Art. 20 is regarded as lex specialis to the right to freedom of expression, as laid down in Art. 19 ICCPR.[20] An example of illegal content featured within IOs are the claims, especially at the start of the pandemic, blaming certain ethnic or national groups for the coronavirus disease, accompanied by incitement to violence towards members of these groups.[21]

(b) IOs that may be prohibited by states. Beyond absolutely prohibited IOs, international law also allows states to prohibit other categories of speech that are capable of causing certain types of harm. For such limitations of speech to occur, there must be (i) a sufficiently clear legal basis, (ii) the pursuit of a legitimate aim, (iii) necessity (in the sense of the least restrictive measure possible) as well as (iv) proportionality *stricto sensu* (i.e., the limitation must be proportionate to the importance of the interest or right protected). Under the ICCPR, the legitimate aims for limiting freedom of expression are a) 'respect of the rights or reputations of others' and b) 'the protection of national security or of public order *(ordre public)*, or of public health or morals.'[22] Regional human rights instruments have their own provisions for limitations of freedom of expression.

In Brzeziński v. Poland, the European Court of Human Rights explicitly referred to the phenomenon of 'fake news'. It did so in the context of local elections in Poland and a statement made by a candidate for a local government position towards the outgoing local administration. In particular, the Court considered Poland's election law which allows a court, within 24 hours, to consider whether certain published information qualifies as 'untrue', and, if so, to issue an order prohibiting its further distribution. While a violation was found on the basis of the procedure before the Polish courts and the sanction imposed,

20 serious of crimes - UNGA Res A/74/486, para. 8.
Human Rights Committee, General comment No. 34. Article 19: Freedoms of opinion and expression, 12 September 2011, CCPR/C/GC/34, para. 51.
21 'Far right using coronavirus as excuse to attack Asians, say police' (The Guardian, 29 August 2020), available at: <https://www.theguardian.com/society/2020/aug/29/far-right-using-coronavirus-as-excuse-to-attack-chinese-and-south-east-asians>
22 ICCPR, Art. 19.

the European Court recognised the necessity of combatting the dissemination of false information on electoral candidates in view of retaining the integrity of the public debate.[23]

The European Union draws a line between 'illegal content' and false claims that are not necessarily illegal. Under European Commission Recommendation 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online, examples of illegal content include child pornography and terrorist propaganda. But the Recommendation's definition of 'illegal content' is otherwise quite broad: 'any information which is not in compliance with Union law or the law of a Member State concerned'.[24] Part of the Recommendation's covered content overlaps with content that the ICCPR requires states to prohibit. For illegal content under the Recommendation, the EU outlined a notice-based procedure for the assessment of content by hosting providers.[25]

Great care is needed in calibrating state responses to disinformation. After all, the measures taken by the state are aimed at a speech act, and free speech is itself protected under international human rights law. As affirmed by the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, 'the human right to impart information and ideas is not limited to "correct" statements, that the right also protects information and ideas that may shock, offend and disturb'.[26] There are several reasons for caution. First, state

23 Brzeziński v. Poland, ECtHR, Judgment of 25 July 2019, para. 55.
24 Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online, Official Journal of the European Union, L 63/50, Chapter I, 4(b).
25 id.
26 Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda, United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human

regulation of disinformation can become a powerful silencing tool in the hands of authoritarian regimes.[27] Second, state regulation that mandates certain rapid assessment and takedown procedures for online intermediaries may relegate decisions impacting human rights to actors that are ill-suited for this task.[28] Third, overly restrictive sanctions or punishment can have a negative impact on the freedom of speech. For intermediaries, heavy fines and other forms of intermediary liability may incentivise them to err on the side of taking down content.[29] For individuals, criminal sanctions can have a chilling effect.[30]

This brief survey suggests a number of conclusions. First, the protective measures required under international human rights law vary according to the type of content in which the false claim is found. This requires careful unpacking of different types of IOs. For manipulated claims used to incite violence, for example, the state is under an obligation to prohibit them. For other types of disinformation that may cause harm, the state is entitled to restrict freedom of speech if the harm falls within one of the 'legitimate aim' categories provided for under international human rights instruments, and only if the restriction is provided by law, necessary and proportionate. Invasive measures, including content takedowns and sanctions, can only be taken in accordance with this test. That said, we need to focus more on the range of measures that states can take to prevent and mitigate the impact of disinformation operations, such as early threat detection, fact-checking, building awareness and resilience within the population, including through training to detect manipulation.

---

and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, available at: <https://www.osce.org/files/f/documents/6/8/302796.pdf>.

27 Caroline Lees, 'Fake News – The Global Silencer' (2018), available at: <https://journals.sagepub.com/doi/pdf/10.1177/0306422018769578>.

28 Article 19, Internet intermediaries: Dilemma of Liability (2013 report), available at: <https://www.article19.org/data/files/Intermediaries_ENGLISH.pdf>.

29 Monica Horten, 'Liability and responsibility: new challenges for Internet intermediaries' (LSE Blog, 20 October 2016), available at: <https://blogs.lse.ac.uk/medialse/2016/10/20/liability-and-responsibility-new-challenges-for-internet-intermediaries/>.

30 McGonagle, "Fake News': False fears or real concerns?' (2017) 35(4) Netherlands Quarterly of Human Rights.

Questions for discussion:

a. What is the scope of the 'foreseeability' and 'life-threatening harm' standards articulated by the Human Rights Committee in its General Comment 36 on the right to life? How proximate must the harm to life or other human rights be to trigger an obligation to respect or protect?

b. What is the standard of care regarding the accuracy of information originating from state actors? According to the 2017 Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda, the protection of free expression, even when it contains a falsity, 'does not justify the dissemination of knowingly or recklessly false statements by official or State actors'.[31] How can official statements be assessed in circumstances where there are no reliable standards for what is true and what is false? This would be particularly relevant in the context of rapidly evolving events that are difficult to assess – for instance, the changing advice on social distancing and the wearing of masks that has occurred during the covid-19 pandemic.

c. Are human rights bodies approaching the balancing test between freedom of expression and the other legitimate interest at stake differently depending on the type of speech? Are there different balancing tests, or at least different tests for assigning weight to the various relevant factors across regional human rights systems?

d. What are the guarantees that must be respected under international human rights law when states impose duties of care on online intermediaries? What types of appeal mechanisms should be in place, and should they be confined to remedies sought by the intermediary?

e. Can and should content moderation decisions that affect users' freedom of expression be, through domestic regulation or otherwise delegated to decentralised online intermediaries? If so, what would this entail for the structure, resources and expertise of these intermediaries? Would

31 Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda, United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, available at: <https://www.osce.org/files/f/documents/6/8/302796.pdf>.

international human rights law obligations binding on states necessitate greater transparency, effectiveness and state oversight of intermediaries' decision-making processes?[32]

f. To what extent are 'political speech' and 'debate on questions of public interest' to be distinguished from other forms of expression? In the area of 'political speech', Schmitt and Milanovic note that 'the mere fact that it is a politician who engages in COVID-19 misinformation, offline or online, does not mean that such speech can never be limited. Unlike First Amendment doctrine, international human rights law does not categorically ban content or viewpoint-based restrictions on political speech.'[33] While it is true that restrictions are not ruled out, the European Court of Human Rights has consistently noted 'that there is little scope under Article 10 § 2 of the Convention for restrictions on political speech or on the debate of questions of public interest'.[34]

g. What is the difference in protection for those who have created the content and those who have further disseminated it, for instance through retweets, reposts or forwards?

h. What, if any, is the relevance of the falsity of the information? Does an emphasis on intention and manipulation overcome any difficulties in assessing the accuracy of a piece of information?

2. Information operations with a transnational element

a. International human rights law: issues of extraterritorial application

In the previous section, we outlined some of the substantive issues that arise under international human rights law in the context of IOs. In this section, we turn to IOs with a transnational element, and address the sharp-end issue for the application of international human rights law to such operations – the concept of extraterritorial jurisdiction.

32 ee, in this direction, David Kaye, 'A New Constitution for Content Moderation', available at: <https://onezero.medium.com/a-new-constitution-for-content-moderation-6249af611bdf>.
33 Schmitt and Milanovic, pp. 276 – 277.
34 Castells v. Spain, para. 43; Wingrove v. the United Kingdom, para. 58.

In the context of human rights treaties, 'jurisdiction' delineates the scope of a state's power and responsibility over individual rights. Indeed, a state can only be required to respect, protect and ensure the human rights over which it has effective control. To this extent, jurisdiction is a trigger to many human rights treaty obligations. Jurisdiction under international human rights law is primarily territorial, covering a state's own territory. Likewise, if a state exercises effective control over territories or areas abroad, jurisdiction also extends to those geographically defined spaces.

Beyond this spatial conception, jurisdiction may be established on the basis of physical control or authority over individual right-holders.[35] This is what is known as the 'personal' model of extraterritorial jurisdiction and most human rights bodies and commentators agree that it applies to both negative and positive human rights obligations, at least in some circumstances.[36] Specifically, this model applies to the extent that control over individuals may be exercised through the activities of state agents abroad, whether to respect, protect or ensure at least the human rights implicated in the situation.[37]

Several human rights bodies have also expressed the view that jurisdiction extends extraterritorially through the activities of entities, such as companies, which are incorporated or located in a state's territory or are otherwise subject to its control. This model focusses on the extraterritorial effects of personal control: jurisdiction covers the activities of the said entities when these have a direct and reasonably

35 HRC, General comment no. 31 [80], The nature of the general legal obligation imposed on States Parties to the Covenant, CCPR/C/21/Rev.1/Add.13, 26 May 2004, § 10.
36 Milanovic, Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy (2011), at 119. But the ECtHR has been reluctant to recognize this model in relation to extraterritorial kinetic force in the absence of governmental control (see ECtHR, Banković and others v. Belgium and others, Appl. no 52207/99, Decision of 12 December 2001, paras 74-82; and ECtHR, Al-Skeini and others v. United Kingdom, Appl. no 55721/07, Judgment of 7 July 2011, paras 136-137). For a recent analysis, see Milanovic, 'The Murder of Jamal Khashoggi: Immunities, Inviolability and the Human Right to Life', 20 Human Rights Law Review (2020) 1, at 23-24.
37 See e.g. Inter-American Commission on Human Rights (IAComHR), Coard et al. v. United States, Report N. 109/99, 29 September 1999, para 37; Al-Skeini, supra note 6, paras 136-139.

foreseeable impact on the human rights of individuals extraterritorially.[38] As such, a state's positive duties concern the rights that may be infringed by said private entities.[39] While endorsed by the Human Rights Committee and the Inter-American Court of Human Rights, other human rights bodies have not endorsed it.[40]

Lastly, the Human Rights Committee has advanced a more expansive approach to extraterritorial jurisdiction, grounded in the exercise of control *over the enjoyment of the rights in question*, regardless of any physical control over territory, the perpetrators, or the individual victim.[41] It bears noting that other human rights bodies have been less enthusiastic about this expansive approach, as evidenced in the recent Georgia v Russia (II) judgement of the European Court of Human Rights.[42] Nonetheless, this functional approach to jurisdiction[43] has been widely accepted in respect of negative human rights duties under the ICCPR.[44] However, many oppose its applicability to positive human rights

38 HRC, Human Rights Committee, General comment No. 36 (2018) on article 6 of the International Covenant on Civil and Political Rights, on the right to life, CCPR/C/GC/36, 30 October 2018, § 22, with respect to the right to life; CESCR, General Comment No. 14 (2000), The right to the highest attainable standard of health (article 12 of the International Covenant on Economic, Social and Cultural Rights), E/C.12/2000/4, 11 August 2000, § 39; CESCR, General Comment No. 15: The Right to Water (Arts. 11 and 12 of the Covenant), UN Doc E/C.12/2002/11, 20 January 2003, § 33; CESCR, Statement on the Obligations of States parties regarding the corporate sector and economic social and cultural rights, UN Doc E/C.12/2011/1, 20 May 2011, § 5; IACtHR, Advisory Opinion OC-23/17 of November 15, 2017 Requested by the Republic of Colombia: The Environment and Human Rights, 15 November 2017, paras 101-102. See also Milanovic and Schmitt, supra note 3, at 29-30.

39 See Besson, Due Diligence and Extraterritorial Human Rights Obligations – Mind the Gap!', 9:1 ESIL Reflections (2020) 2, at 2.

40 HRC, General Comment 36 (n 38) para. 22; CESCR, 'Statement on the Obligations of States parties regarding the corporate sector and economic social and cultural rights', UN Doc E/C.12/2011/1, 20 May 2011, para. 5; IACtHR, Advisory Opinion OC-23/17 of November 15, 2017 Requested by the Republic of Colombia: The Environment and Human Rights, 15 November 2017, paras 101-102. See also Milanovic and Schmitt, p. 264-265

41 HRC, General Comment 36, supra note 8, § 63.

42 ECtHR, Georgia v Russia (II), App. No. 38263/08, Judgment of 21 January 2021, paras. 117 – 144.

43 See Shany, 'Taking Universality Seriously: A Functional Approach to Extraterritoriality in International Human Rights Law', 7 The Law & Ethics of Human Rights (2013) 47.

44 Milanovic, Extraterritorial Application, supra note 6, at 209; Goodman, Heyns and Shany, Human Rights, Deprivation of Life and National Security: Q&A with Christof Heyns and Yuval Shany on General Comment 36 (2019), available at https://www.justsecurity.org/62467/human-life-national-security-qa-christof-heyns-yuval-shany-general-comment-36/, at 1-2; HRC, Sergio Euben Lopez Burgos v Uruguay, Human Rights Committee (HRC) Communication No 52/1979, UN Doc CCPR/C/13/D/52/1979, 29 July 1981, § 12.3; Lilian Celiberti de Casariego v Uruguay, HRC Communication No

obligations, fearing the lack of necessary governmental infrastructure or powers beyond a state's territory or spatial control.[45] Such concerns tend to overlook the modest import of positive human rights duties, which extend only insofar as the duty-bearer has the capacity to adopt the protective measures in question.[46] Capacity, in this context, includes the ability to influence the behaviour of the perpetrators,[47] the unpredictability of certain events, the availability of resources, the duty to respect and protect other human rights, and other international obligations.[48] Thus, states are not required to do the impossible or to discharge a 'disproportionate burden',[49] but are expected to adopt measures that are available and reasonable in the circumstances.[50]

When it comes to IOs taking place on social media or other virtual platforms, such as private messaging applications, the challenge is how to establish jurisdiction over acts occurring in 'cyberspace' or the so-called 'cyber domain'. But these misnomers should not derail the existing debate. After all, online activities do not occur in a separate, virtual space which entities cannot grasp or control, and where individuals cannot be harmed. Quite the contrary: such activities are online because they occur through the Internet and other information and communications technologies (ICTs) and pervade the existing

56/1979, UN Doc CCPR/C/13/D/56/1979, 29 July 1981, para 10.3; ECtHR, Issa and others v. Turkey, Appl. no. 31821/96, Judgment of 16 November 2004, para 71.

45 See, e.g., the account of the debate in Milanovic, The Murder of Jamal Khashoggi, supra note 6, at 19-20; and Milanovic, Extraterritorial Application, supra note 6, at 209, 210-212, 219-220.

46 For example, the ICESCR has no express jurisdictional threshold and yet most of its obligations are positive ones, i.e. duties to protect and ensure social, economic and cultural human rights.

47 Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro), Judgment, 26 February 2007, ICJ Reports (2007) 43, para 430.

48 Cf. ECtHR, Osman v. United Kingdom, 87/1997/871/1083, Judgment of 28 October 1998, para 116.

49 Ibid.; see also ECtHR, Nicolae Virgiliu Tănase v. Romania, Appl. no. 41720/13, Judgment of 25 June 2019, para 136.

50 ECtHR, McCann and Others v. United Kingdom, Appl. no. 19009/04, Judgment of 27 September 1995, para 151; IACtHR, Velasquez Rodriguez v. Honduras, Judgment (Merits), 29 July 1988, para 167. See also The Netherlands, Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace — Appendix: International law in cyberspace (2019), at 4; and Republic of Korea, Comments on the pre-draft of the OEWG Report (2020), at 5.

domains of land, sea, air and outer space. In doing so, they cross multiple national borders to ultimately affect real individuals. ICTs are not only made up of software and data, but also hardware devices and the persons behind them, all of which can be subject to effective state control. Thus, while the territorial, spatial and personal models of jurisdiction may cover certain forms or aspects of IOs (provided a state has physical control over the hardware used or the right-holders in question), the functional model would comprehensively capture all dimensions of the phenomenon.

Questions for discussion:

a. How much physical control of spaces, persons and objects is involved in an IO?
b. What jurisdictional model is best suited to cover IOs?
c. How much state and scholarly support is there for the functional approach to human rights jurisdiction?
d. Does the concept of human rights jurisdiction refer to the individual rights-holder or the human right(s) in question?

b. Principle of non-intervention

Each state should be able to conduct its affairs without outside interference.[51] The rule of non-intervention prohibits interference that bears 'on matters in which each state is permitted, by the principle of state sovereignty, to decide freely' and uses methods of coercion in regard to such matters.[52] According to the International Court of Justice in Nicaragua, 'the element of coercion [...] forms the very essence of prohibited intervention'.[53] Yet there is little clarity over its the definition. As the Netherlands acknowledged in a 2019 statement – 'the precise definition of coercion, and thus of unauthorised intervention, has not yet fully crystallised in international law.'[54]

51 Nicaragua case, para. 202.
52 Ibid, para. 205.
53 Nicaragua, para. 205.
54 Letter to the parliament on the international legal order in cyberspace, available at: <https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-in-

According to the Dutch statement, coercion, at its core, 'means compelling a state to take a course of action (whether an act or an omission) that it would not otherwise voluntarily pursue. The goal of the intervention must be to effect change in the behaviour of the target state.' Although the change in the course of action, or in the availability of courses of action, may be clearer in cases of meddling with voting machines or tabulation software, it seems less apparent in other IOs. This is due to the need for a line distinguishing between IOs that are not seen as prohibited under international law, and coercive IOs that are.

Taking voluntary pursuit of a course of action as a starting point, and linking it to the deprivation of meaningful choice, Wheatley argues that IOs, when they deceive individuals of the reality of the situation through the provision of false facts, may qualify as coercive.[55] As an example of such operations, he discusses the circulation of a deep fake, leading individuals to vote for another candidate – something they would not have done had it not been for the deception created through the deep fake content. Wheatley concludes that

> Fake news is "coercive" when the communication is intended to deceive the target population into doing something they would not otherwise have done, absent the false information.[56]

From this, it may be argued that to coerce is to seek to effect a change in the behaviour of the targeted state, a change that would not occur but for the actions of the intervening state. As such, coercion could be applied not only through force, violence or threats but also deception.

A state's sovereign choices presume the exercise of free will. In addition to a change in the victim's behaviour, the current understanding of coercion seems to imply an element of intentionality or purpose. For instance, the Netherlands stated that 'intervention is defined as

ternational-legal-order-in-cyberspace>.
55 Steven Wheatley, 'Cyber and Influence Operations Targeting Elections: Back to the Principle of Non-Intervention' (EJIL:Talk!, 26 October 2020).
56 Id.

interference in the internal or external affairs of another state with a view to employing coercion against that state.'[57] Similarly, Wheatley speaks of an intention to deceive underlying the act of intervention in influence operations. The existence of an element of intentionality, as well as the type of intentionality involved, is of particular importance here. This creates a basis for differentiating between operations aimed at circumscribing the choices of the targeted states and operations that have this effect, but which are aimed at achieving something else (for instance, an information-gathering operation that incidentally compromises a system for the delivery of a vaccine).

Finally, one could argue that the line delineating a prohibited intervention from permitted interference turns on the character of the information being distributed through the IO, and more precisely on whether it is accurate or false. This line is consistently drawn in the literature. For instance, Wheatley argues that 'the principle that "just providing the facts" is not a violation of the non-intervention rule applies equally to information gained by hacking computer systems and making that information public, with the objective of influencing political debates.'[58]

Yet one could very easily imagine the dissemination of accurate information, especially confidential or sensitive data, selected and presented in a particular way, and with the requisite intention, that could have a significant influence on the public, even (under certain interpretations) satisfying the criterion of coercion. In such cases, there is no manipulation of the content of the information, but a form of manipulation is apparent in the content's selection, delivery, timing and target audience. A clear difficulty with this element is that one runs into the challenges of separating true and false information.

57 Letter to the parliament on the international legal order in cyberspace, available at: <https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace>. Emphasis added.
58 Steven Wheatley, 'Cyber and Influence Operations Targeting Elections: Back to the Principle of Non-Intervention' (EJIL:Talk!, 26 October 2020).

c. Sovereignty

In recent years, a number of states[59] have asserted that respect for sovereignty is a self-standing rule of international law, the breach of which, when attributable to a state, would constitute an internationally wrongful act.

According to Schmitt and Milanovic, 'the sovereignty of a state may be breached by cyber operations attributable to another state in two basic ways – by causing effects on the territory of the former or by interfering with its inherently governmental functions, even in the absence of territorial effects.'[60] On the first way, the Tallinn Manual 2.0 posits that relatively permanent interference with the functionality of cyber infrastructure would qualify as 'effects' or 'consequences' for the purposes of the rule.[61] On the second, we are looking at interference with, or usurpation of an inherently governmental act. While healthcare or cybersecurity, for example, are not necessarily governmental functions across jurisdictions, crisis management and national security, including in the context of infectious disease, are.[62] The conduct of elections is a paradigmatic example of such a function.

Part of the appeal of the rule of sovereignty is that it may circumvent the difficulties associated with defining 'coercion' in the rule of non-intervention. However, this rule comes with its own challenges. Two main issues arise around the rule of sovereignty. First, its existence as a self-standing rule of international law is still in doubt.[63] Second, the

59 See, for instance, the Netherlands (Letter of July 5, 2019 from the Netherlands Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace, Appendix: International Law in Cyberspace 2, https://perma.cc/ENU3-DFGV), France (Ministry of the Armies, International Law Applied to Operations in Cyberspace 6-7 (2019)), Statements of Austria, Finland and the Czech Republic at the 2d Substantive Session of OEWG, Feb. 11, 2020, https://perma.cc/J269-SU36.

60 p. 253

61 Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Michael N. Schmitt gen. ed. 2017), pp. 20 – 21.

62 Schmitt and Milanovic, p. 255.

63 The United Kingdom is opposed to this rule and has forcefully rejected its existence for a number of years: Jeremy Wright, Attorney General of the UK, Address at Chatham House, Cyber and International

boundaries of the rule are unclear. In 2020, the General Counsel of the United States Department of Defense, Paul Ney, opined that not 'all infringements on sovereignty in cyberspace necessarily involve violations of international law'.[64] At the same time, France takes a very broad view of this rule: 'any cyberattack against French digital systems or any effects produced on French territory by digital means by a State organ, a person or an entity exercising elements of governmental authority or by a person or persons acting on the instructions of or under the direction or control of a State constitutes a breach of sovereignty.'[65]

d. Principle of self-determination

Jens Ohlin[66] and Nicholas Tsagourias[67] have argued that IOs during electoral processes may be prohibited under the rule of self-determination, which protects the right of people to freely choose their political status without outside interference.[68] Under this view, what is crucial is not the content of the IO, but the identity of the perpetrator. The real harm in these operations lies in cases where an outsider is posing as an insider.

e. The Corfu Channel and the No-harm principles

Transboundary IOs may also fall within the scope of two related but distinct rules requiring states to exercise due diligence in preventing, halting and/or redressing certain types of harm. The first of these rules is the Corfu Channel principle, which borrows its name from the (first) case decided by the International Court of Justice back in

Law in the 21st Century (May 23, 2018).
64 Paul C. Ney, Jr., Department of Defense General Counsel, DOD General Counsel Remarks at U.S. Cyber Command Legal Conference (Mar. 2, 2020).
65 Ministry of the Armies, International Law Applied to Operations in Cyberspace 6-7 (2019). Emphasis added.
66 Jens D Ohlin, 'Did Russian Cyber-Interference in the 2016 Election Violate International Law?' (2017) 95 Texas Law Review 1579.
67 Nicholas Tsagourias, 'Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace' (EJIL: Talk!, 26 August 2019), available at: <https://www.ejiltalk.org/electoral-cyber-interference-self-determination- and-the-principle-of-non-intervention-in-cyberspace>.
68 Declaration on Principles of International Law Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, UNGA Res. 2625 (XXV), 24 October 1970.

1949, between the UK and Albania. There, the Court found that it is a 'well-recognized principle' that every state has an 'obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States.'[69] To the extent that IOs may be carried out by states or non-state actors and contravene the victim state's right to sovereignty, non-intervention, self-determination, or the human rights of its population, they may well be covered by the Corfu Channel principle. This means that a state from whose territory or physical infrastructure the IO is carried out must exercise its best efforts to prevent or stop the operation from undermining the rights of other states.

The second rule requiring states to exercise due diligence is the no-harm principle. It requires states to prevent, stop and redress significant transboundary 'harm to persons, property or the environment'.[70] Failure to exercise due diligence gives rise to liability to compensate the harm once it materialises.[71] It is only when this liability is not met that international responsibility arises. While there is no question that this principle applies beyond the ecological context,[72] controversy remains as to whether it is limited to physical harm or extends to non-physical damage, such as moral, financial and reputational harm.[73] But controversies over its scope aside, it is beyond doubt that states must prevent, halt and redress significant transboundary harm to the life, health or physical integrity of individuals caused by IOs.

69 Corfu Channel Case (United Kingdom v Albania), Judgment, 9 April 1949, ICJ Reports (1949) 4, at 22
70 ILC, Draft articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries, in Report of the International Law Commission on the work of its fifty-third session (23 April–1 June and 2 July–10 August 2001), UN Doc. A/56/10, at 152-153, Article 2(b) and Commentary, paras 8 and 9
71 ILC, Draft Articles on Prevention, at 148, General Commentary, para 1; at 150, Commentary to Article 1, para 6
72 Fourth report on international liability for injurious consequences arising out of acts not prohibited by international law, by Mr. Robert Q. Quentin-Baxter, Special Rapporteur', UN Doc. A/CN.4/373 and Corr.1&.2, 27 June 1983, para 17.
73 ILC, Draft Articles on Prevention, at 151, Commentary to Article 1, para 16.

Questions for discussion:

a. What is the content of 'coercion' in the prohibition of intervention?

b. Does the veracity of the information underlying an IO have any bearing on the rule of non-intervention?

c. Is there an evolving consensus around a rule of sovereignty applicable to ICTs (which the UK has been reluctant to accept)?

d. What is the content of this rule when it comes to IOs? In particular, to what extent do breaches of confidentiality, integrity and availability of data and systems arising from an IO amount to a violation of sovereignty? Can an IO violate sovereignty if the harm it causes does not involve a loss of functionality or a usurpation of inherently governmental functions?

e. Does the principle of self-determination relate only to foreign IOs or can it protect a people against an IO from their own government?

f. What types of physical and non-physical harm caused by an IO might fall within the scope of the Corfu Channel and no-harm principles? What standard of due diligence do these rules require from states in the IO context?

III. Does International Law Need Clarification or Development with respect to IOs?

As shown in the previous sections, international law contains a range of obligations that regulate the conduct and effects of IOs. However, difficulties remain. We will limit our observations to some of the existing challenges in analysing IOs under an international law framework.

(a) There are relatively few tailor-made international law rules for IOs and those that exist are specific to particular contexts (e.g., incitement to genocide, racial or religious violence).

(b) Inter-state obligations, such as non-intervention and sovereignty may prohibit certain IOs, just as the Corfu Channel and no-harm principles may require states to exercise due diligence to prevent or end them.

But significant interpretative challenges remain. These interpretative challenges bring a degree of uncertainty in the application of these rules to specific IOs.

(c) These challenges are exacerbated in the IO context where operations drive towards cognitive effects rather than physical outcomes.

(d) International human rights law offers a promising set of obligations for IOs, including (i) the right to life, freedom from ill-treatment and health, (ii) voting, public participation, and public service, (iii) freedom of expression, (iv) freedom of thought, (v) the right to privacy, and (vi) self-determination.

- It both prohibits state action that violates human rights and requires states to ensure its own citizens are protected from human rights violations by third parties.

- It clearly governs what states do internally and, depending on the appropriate approach to extraterritoriality, may restrict state interference with the human rights of people abroad. That said, the extraterritoriality problem looms large, and to the extent it applies to all human rights issues, is unlikely open to an easy resolution in the IO context.

Looking across these issues, there are multiple areas where existing international law could benefit from further clarification or elaboration with respect to IOs, such as:

- The prohibition of 'domestic IOs', whereby states spread misinformation, disinformation or malinformation about its own electoral processes or other matters involving the basic rights of their citizens (e.g., pandemic response);

- The duty to prevent transboundary harms to life, health and other human rights caused by IOs emanating from a state's territory;

- The elements of the prohibition of intervention, and in particular the relationship between the means and effects of IOs and the concept of 'coercion'.

Separately, there are also several areas where international law might benefit from new international legal rules, standards, or principles. Possibilities include:

- A prohibition on IOs that incite a violation of any rule of international law/an internationally wrongful act (recalling that international law only prohibits incitement to genocide, racial, or religious violence);

- A prohibition on IOs that cause serious adverse consequences to other states;

- A prohibition on IOs that use certain means and methods (for instance, deception with respect to the identity of the author or the use of bots in generating or spreading content).

Foreign Influence Campaigns and the Non-Intervention Principle

Steven Wheatley*

* Professor of International Law, University of Lancaster

The objective here is to explain how the non-intervention principle can regulate foreign State cyber influence operations, i.e. influence operations conducted using information and communications technologies (ICTs). The presentation is structured as a series of Propositions in order to establish as much common ground as possible – and locate points of disagreement for further discussion. The analysis draws on arguments made in Wheatley, 'Foreign Interference in Elections under the Non-Intervention Principle: We need to Talk about "Coercion"' (2020) 31 Duke Journal of Comparative & International Law 161.[1]

Proposition 1: The non-intervention principle prohibits one State from intervening in the domestic political affairs of another State.

Reasoning:

The non-intervention principle is a rule of customary international law.[2]

The clearest expression of the content of the rule can be found in paragraph 205 of the ICJ's 1986 Nicaragua judgment:

> 'A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely… Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones.'

There are 3 component elements to the non-intervention rule:

1. The non-intervention principle concerns actions attributable to a State.

1 See, also, Wheatley, 'Cyber and Influence Operations Targeting Elections: Back to the Principle of Non-Intervention', EJIL: Talk! October 2020.
2 Military and Paramilitary Activities in and against Nicaragua, (Nicaragua v. United States of America), Merits, Judgment [1986] ICJ Rep 14, para. 202.

2. The action must be aimed at interfering in a matter that the target State should be permitted to decide freely, including the composition of the Government and policy choices.

3. Intervention is wrongful when it uses methods of coercion.

Proposition 2: A State can intervene by words and other forms of messaging.

Reasoning:

The notion of intervention includes intervention by words and other forms of messaging (e.g. images and videos). This is seen, for example, in the long-standing prohibition on 'subversive intervention' under customary international law.[3] Subversive interventions are propaganda operations that use words and other forms of messaging, with the objective of destabilizing the target State by influencing its nationals towards insurrection or revolt.[4]

Foreign state influence operations, in the form of news stories, opinion pieces, and other forms of communication, are unlawful where they can be categorized as 'subversive interventions', or the influence operation can be categorized as 'coercive' (following the logic of the 1986 Nicaragua judgment).

Proposition 3: The target of a prohibited intervention can be the Government, the political class, including Opposition political parties, or the citizens of the State.

3 Emer de Vattel, The Law of Nations [1797] (Liberty Fund, 2008), Book II, Ch IV, para. 56. See, also, Quincy Wright, 'Subversive Intervention' (1960) 54 American Journal of International Law 521.
4 See Philip Kunig, 'Intervention, Prohibition of' (2008) Max Planck Encyclopedia of Public International Law, para. 24; and Eric de Brabandere, "Propaganda" (2012) Max Planck Encyclopedia of Public International Law [online], para. 10.

Reasoning:

In order to get 'a State' to do something that it would not otherwise do, the outside power can target the Government, in the form of its senior Ministers:

> E.g., when the President and Foreign Minister of Czechoslovakia were subjected to 'third-degree methods of pressure' by Nazi officials in 1939, Czechoslovakia was coerced into agreeing to the establishment of a German protectorate over Bohemia and Moravia.[5]

The foreign State can also get the target State to do something that it would not otherwise do by changing the Government:

> E.g. Operation Storm-333, of 27 December 1979, which saw special forces from the Soviet Union replace Afghan President Hafizullah Amin with Babrak Karmal.[6]

The outside can also seek to maintain the status quo by undermining Opposition political parties.

Finally, the foreign power can get the target State to do something that it would not otherwise do by directly influencing the citizens of the State, by calling on the population to vote in a particular way in an election, or a referendum:

> E.g., in the 2016 Brexit referendum, President Barack Obama warned the British public that the UK would be at the "back of the queue" in any trade deal with the US, if the UK chose to leave the European Union.[7]

The line between an unwelcome interference, and unlawful intervention is established by the criterion of 'coercion'. Thus, if a foreign power threatened a military invasion, if the population voted a certain way in an

5 See Yearbook of the International Law Commission (1966), vol. II, p. 246.
6 General Assembly resolution ES-6/2, 'The situation in Afghanistan and its implications for international peace and security', adopted 14 January 1980, by 104 votes to 18, 18 abstaining.
7 Anushka Asthana and Rowena Mason, "Barack Obama: Brexit would put UK "back of the queue" for trade talks", The Guardian, 22 April 2016.

election, this would clearly be coercive and wrongful under the principle of non-intervention.

Proposition 4: The non-intervention principle applies in the cyber domain.

Reasoning:

There is widespread agreement that international law regulates the use by States of information and communications technologies (ICTs).[8] This means that rules that apply in the physical world also apply in the domain of cyber, including the principle of non-intervention.[9]

Proposition 5: The application of the non-intervention principle to State use of ICTs depends on our understanding of the term 'coercion'.

Reasoning:

There is presently no agreement on which state cyber operations can be categorized as 'coercive'. The Government of the Netherlands explains the point this way:

> 'The precise definition of coercion, and thus of unauthorised intervention, has not yet fully crystallised in international law. In essence it means compelling a state to take a course of action (whether an act or an omission) that it would not otherwise voluntarily pursue. The goal of the intervention must be to effect change in the behaviour of the target state.'[10]

8 Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report, UN Doc. A/AC.290/2021/CRP.2, 10 March 2021, para. 34 ("States were called upon to avoid and refrain from taking any measures not in accordance with international law… States also concluded that further common understandings need to be developed on how international law applies to State use of ICTs").

9 Open-ended working group on developments in the field of information and telecommunications in the context of international security, Chair's Summary, A/AC.290/2021/CRP.3, 10 March 2021, para. 11 ("Specific principles of international law which were reaffirmed include… non-intervention in the internal affairs of other States").

10 Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace ("Attempts to influence election outcomes via social media are [covered by] the non-intervention principle."); Australia has adopted a similar position "A prohib-

In order to make sense of the cyber non-intervention principle, we have to unpack the notion of 'coercion.'

Proposition 6: There is a basic structure underpinning the notion of 'coercion'.

Reasoning:

The standard example of 'coercion' is threat by the Robber to his Victim, "Your money or your life." This can be formulated in the following way: the Robber wants his Victim to do something, and wants to be certain that this will happen; the Robber issues a threat that his Victim cannot reasonably refuse; and because of the threat, the Victim hands over the money.

We can, then, formulate the notion of 'Coercion' as follows:

> (1) One actor ('P') wants another actor ('Q') to do something ('X'), and wants to be certain that Q will do X – it is this second element that distinguishes coercion and other efforts to exercise power, from the mere exercise of influence;[11]
> (2) P then takes some action to get Q to do X; and
> (3) because of P's actions, Q does X.

Coercion describes a situation, then, when one actor ('P') takes some action to ensure that another actor ('Q') does something (or does nothing) (i.e. 'does X').

Proposition 7: There is a violation of the principle of non-intervention when State use of ICTs to influence the process of political decision-making in another State uses methods of coercion.

---

ited intervention is one that interferes by coercive means (in the sense that they effectively deprive another State of the ability to control, decide upon or govern matters of an inherently sovereign nature)": 2019 Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace.
11 See Joel Feinberg, Harm to Self (Oxford: Oxford University Press, 1986), p. 189.

Reasoning:

Proposition 7 follows logically from Proposition 1 (The non-intervention principle prohibits one State from intervening in the domestic political affairs of another State); Proposition 2 (A State can intervene by words and words and other forms of messaging); and Proposition 4 (The non-intervention principle applies in the cyber domain).

Proposition 7 makes clear that a violation of the non-intervention rule does not require evidence of a successful intervention. The International Court of Justice in the 1986 Nicaragua case was not concerned with the success of the United States' intermeddling in Nicaraguan internal affairs judgment. The ICJ made the point that 'intervention is wrongful *when it uses methods of coercion*'.[12]

The focus of attention is on the foreign power: There is a violation of the non-intervention rule when (1) State P wants State Q to 'Do X,' and wants to be certain that this will happen; and (2) State P takes some action in order to get the political system in State Q to 'decide' to 'Do X', either by changing (or maintaining) the Government, or changing (or maintaining) a policy position (it does not matter whether State Q "Does X," or not.)

Proposition 8: Lies and deceptive forms of messaging can be a method of coercion.

The notion of coercion, as we have seen, describes a situation in which one actor ('P') takes some action to ensure that another actor ('Q') does something (or does nothing). One way this can be done is by lying.

Consider the following examples:

> **Example 1:** State P wants to supress voter turnout in a key electoral ward in State Q. On election day, State P releases false social media reports of

12 1986 Nicaragua (Merits) case, para. 205 (emphasis added).

an "active shooter situation" in the ward.[13] This is certain to supress voter turnout: By lying State P achieves its objective of suppressing voter turnout, leaving voters without a meaningful choice as to whether to vote, or not.

Example 2: During a presidential election campaign in State Q, the intelligence agency in State P releases a 'deep fake' video that appears to show, in convincing detail, the sitting President, Jones engaged in sexual acts with a child. This is certain to undermine support for President Jones. Citizens have been deceived into voting differently and have been given no meaningful choice in the matter, because they now have a false perception of the reality of the moral fitness of Jones for high office.

Proposition 9: Disinformation campaigns can be a method of coercion.

Reasoning:

The basic political question in any democracy is What is it that we should do? This is answered by the public at the time of a general election or referendum, and by the governing political class at other times.

Campaigns of disinformation undermine the capacity of the population and political class to make decisions in their own interests, based on reliable information.

Coercion describes a situation in which 'P' takes some action to ensure that the target ('Q') does something (or does nothing). Disinformation campaigns can be coercive in one of two circumstances:

(1) Where there is a sustained campaign of disinformation intended to paralyze the process of political decision-making (i.e. to get the political system in the target State to 'do nothing') by creating confusion about the facts and undermining the faith of the local population in the political system to deliver the best policy outcomes.

(2) Where there is a sustained campaign of disinformation that uses sock puppets to manipulate the domestic policy debate. Here, the objective

13 I have to thank Mike Schmitt for this excellent example.

of the influence campaign is to move the target population to a position which aligns with the interests of the outside power, and to get them to believe that they reached the policy position without outside interference.

Proposition 10: Information campaigns can NOT be categorized as methods of coercion, unless the objective is to overwhelm the information environment with a single political narrative.

Reasoning:

There is widespread agreement in the literature that providing the citizens of another country with factual information, including information critical of the government of that state, does not constitute a prohibited intervention. It follows that genuine news broadcasts by state-owned and state-controlled media do not fall within the definition of an unlawful intervention. The same holds for commentaries on the news. In the same way that attempting to influence another person by 'just providing the facts' is not wrongful, efforts by one state to influence the population of another by providing factual information and commenting on news stories is not wrongful.

This means that the practice of Doxfare is not prohibited under the non-intervention rule. Doxfare involves the hacking of computer systems and putting sensitive information into the public domain, with the intention of influencing the internal affairs (e.g. 'DNC-hack').[14] Doxfare is protected by the general rule that 'just providing the facts' to the citizens of another state – even unlawfully obtained facts – is not prohibited by the principle of non-intervention.

There is one exception to the general rule that just providing the facts does not violate the non-intervention rule.

14 See Ido Kilovaty, "Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information" (2018) 9 Harvard National Security Journal 146.

An influence operation that overwhelms the information environment in the target state can be categorized as coercive—and therefore wrongful—when it drowns out all other political voices, because citizens will not have access to information and opinions from a plurality of sources. In other words, voting becomes meaningless, if citizens think they have only one viable option.

Conclusion

The preceding analysis leads to the following conclusions:

Conclusion 1: There is a violation of the principle of non-intervention when State use of ICTs to influence the process of political decision-making in another State uses methods of coercion.

Conclusion 2: There is NOT a violation of the principle of non-intervention when State use of ICTs to influence the process of political decision-making in another State provides factual information and good faith commentaries on the news.

State use of ICTs to influence the process of political decision-making in another State can include the production of news stories, opinion pieces, and other forms of messaging (including pictures and videos), which are then made publicly available via the Internet (including via social media), and therefore potentially accessible by citizens in other states, with the objective of influence the process of political decision-making in the target State.

The process of political decision-making includes, but is not restricted to, the conduct of elections and holding of referendums, as well as the public policy decision-making by the Government and Opposition politicians and political parties.

Methods of coercion in cyber influence operations include, but are not restricted to: (a) Lies and deceptive forms of messaging; (b) Disinformation campaigns; and (c) Influence operations designed to overwhelm the information environment with a single political narrative. This means that Conclusion 1 can also be formulated as follows:

Conclusion 1(a): There is a violation of the principle of non-intervention when State use of ICTs involves lying and other deceptive forms of messaging in an attempt to decisively influence the process of political decision-making in another State.

Conclusion 1(b): There is a violation of the principle of non-intervention when State use of ICTs involves a sustained campaign of disinformation in an attempt to decisively influence the process of political decision-making in another State.

Conclusion 1(c): There is a violation of the principle of non-intervention when State use of ICTs is intended to create a single political narrative in an attempt to decisively influence the process of political decision-making in another State.

International humanitarian law and the limits of information or psychological operations during armed conflicts

April 2021

*Dr. Tilman Rodenhäuser**

* Dr Tilman Rodenhäuser is a legal adviser at the International Committee of the Red Cross. The views expressed in this paper are those of the author and do not necessarily reflect those of the ICRC.

Contents

I. Introduction

'Information operations' or 'psychological operations' have long been part of armed conflicts. Among Western militaries, they are commonly understood as the employment of communication or other means to influence views, attitudes or behavior of adversaries or civilian populations in order to achieve political and military objectives.[1] Other States consider such operations to be part of 'information warfare', which may be understood as a confrontation of two or more States in information

1 See, for example, République Française, Ministère de la Défense, Manuel de Droit des Conflits Armés, Direction des Affaires Juridiques, Sous-Direction du Droit International et du Droit Européen, Bureau du Droit des Conflits Armés, Édition 2012, p. 68 (cited as French Military Manual); Norwegian Ministry of Defence, Manual of the Law of Armed Conflict, Oslo, 2013, 1st English-language edition 2018, p. 199 (cited as Norwegian Military Manual); NATO, Allied Joint Doctrine for Psychological Operations, AJP-3.10.1, Edition B Version 1, with UK national elements, NATO Standardization Office, September 2014, pp. 1-1 and 1-3; Office of the Chairman of the Joint Chiefs of Staff, DOD Dictionary of Military and Associated Terms, Washington DC, as of January 2020, p. 104. See also Winther, International Humanitarian Law and Influence Operations: The Protection of Civilians from Unlawful Communication Influence Activities during Armed Conflict, PhD Thesis, Uppsala Universitet, p. 41.

space and includes 'undermining political, economic and social systems' and 'psychologically manipulating masses of the population to destabilize society and the State'.[2] With the rapid growth of information and communication technology (ICT) over the past decade, the scale, the speed, the reach and the possible humanitarian impact of information or psychological operations has increased significantly.[3]

Reports suggest that States and non-State armed groups are using digital information or psychological operations for a variety of purposes. For instance, information or psychological operations can serve to give an effective advance warning of an attack or to help direct civilians to safety. But there are also information or psychological operations that are designed to cause confusion or harm. On one end of the spectrum, they include the operations to mislead the adversary or to induce the adversary to act recklessly ('ruses of war'), the propagation of the parties' views or 'narrative' about an armed conflict to influence domestic and international audiences, attempts to discredit other parties to a conflict, or to recruit soldiers or fighters.[4] On the other end, such operations are also used to spread fear and terror among populations or to incite violence.[5] Whether and how digital information or psychological operations can cause harm to humans remains, however, subject to debate: inquiries have cautioned that whether online hate campaigns 'have led or contributed to actual outbreaks of violence is difficult to establish' and needs further examination, while also noting that there is information suggesting that in some contexts 'the linkage between offline and online hate speech and real world acts of discrimination and violence is more than circumstantial'.[6]

2 Member States of the Shanghai Cooperation Organization, Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization, 2009.
3 ICRC, Harmful Information: Misinformation, Disinformation and Hate Speech (MDH) in Conflict and Other Situations of Violence, forthcoming. The report finds: 'High internet speed and availability; social media's omnipresence and access; the use of algorithms and artificial intelligence to "optimise" user experience; and the large, unregulated, easy to access digital environments are all elements that, in conjunction with traditional media and information flows, make MDH more pervasive and powerful today than in the past.'
4 See, for example, Minority Rights Group International, Peoples under Threat 2019; see also Graphika, French and Russian Influence Operations Go Head to Head Targeting Audiences in Africa, 2020.
5 For an overview of reported usages of information operations in contemporary armed conflicts, see Minority Rights Group International, Peoples under Threat 2019.
6 Human Rights Council, Report of the detailed findings of the Independent International Fact-Finding

Given their broad definition, digital information or psychological operations can involve various methods, including propaganda, misinformation, disinformation, and hate speech. Humanitarian organizations have observed that in times of armed conflict or in other situations of violence, digital misinformation, disinformation and hate speech can contribute to harassment, defamation, intimidation, social unrest, displacement, adverse effects on the operations of humanitarian organizations, or to physical violence against particular groups.[7] Such risks are particularly acute if misinformation, disinformation or hate speech are used in periods of instability, including armed conflicts, and/or if it coincides with pre-existing social tensions, low levels of digital literacy, lack of trust or transparency in mainstream media or the authorities.[8]

Information or psychological operations during armed conflicts are not, as such, unlawful. Experts have stressed that many forms of 'propaganda, even disinformation' are unproblematic under IHL[9] and that 'psychological operations directed at the civilian population have been a feature of warfare for centuries'.[10] Some States' military manuals expressly assert the permissibility of information or psychological operations. For example, the German military manual states 'it is permissible to exert political and military influence by spreading – even false – information to undermine the adversary's will to resist and to influence their military discipline (e.g. calling on them to defect, to surrender or to mutiny)'.[11] The French military manual notes that 'the law of armed conflict does not regulate

Mission on Myanmar, Thirty-ninth session, 10–28 September 2018, UN Doc. A/HRC/39/CRP.2, 17 September 2018, paras 1325-6.

7 ICRC, Harmful Information: Misinformation, Disinformation and Hate Speech (MDH) in Conflict and Other Situations of Violence, forthcoming. See also Mercy Corps, The Weaponization of Social Media, 2019.

8 ICRC, Harmful Information: Misinformation, Disinformation and Hate Speech (MDH) in Conflict and Other Situations of Violence, forthcoming.

9 Sassòli and Issar, "Challenges to International Humanitarian Law", in von Arnaud, Matz-Lück and Odendahl (eds), 100 Years of Peace Through Law: Past and Future, Duncker & Humblot, Berlin, 2015. pp. 181-235.

10 Schmitt, France Speaks Out on IHL and Cyber Operations: Part II, EJIL:Talk!, 1 October 2019.

11 Germany Federal Ministry of Defence, Law of Armed Conflict Manual, Joint Service Regulation (ZDv) 15/2, Berlin, May 2013, p. 75 (cited as German Military Manual). See also Canada National Defense, Law of Armed Conflict at the Operational and Tactical Levels, Joint Doctrine Manual, B-GJ-005-104/FP-021, Ottawa, 2001, p. 7-4 (cited as Canadian Military Manual).

psychological operations as such' and that 'non-violent psychological operations are not prohibited and lawful even if targeted at civilians.[12] The United States DoD Law of War Manual asserts that 'in general, the use of propaganda is permissible under the law of war, even when it encourages acts that violate an enemy State's domestic law or is directed towards civilian or neutral audiences'.[13] A number of States further affirm that misinformation or psychological warfare can form part of lawful ruses of war.[14] Importantly, however, these States are also clear that information or psychological operations have well-established limits in existing rules of international law, including international humanitarian law (IHL) and international criminal law.

This paper analyzes the limits that IHL imposes on information or psychological operations during armed conflicts, focusing in particular on those operations that employ digital technology.[15] While other bodies of international law, notably human rights law and international criminal law, may also provide relevant rules, they are outside the scope of this paper.

2. Under IHL, information or psychological operations during armed conflict are not unlimited

In broad terms, IHL contains two types of rules that address information or psychological operations.

First, there are few rules which address directly what may be called information or psychological operations. This category includes, for example, the prohibition of using 'pressure or propaganda which aims at securing voluntary enlistment' of protected persons in occupied

12 French Military Manual, p. 68. (tranlation by the author)
13 US Department of Defence, Law of War Manual, June 2015 (updated December 2016), p. 331 (cited as United States DoD Manual).
14 See, for instance, the excerpts of the Military Manuals of Australia, Ivory Coast, Israel, Nigeria, South Africa, and the United States of America presented here: https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule57
15 This paper is written based on the position that IHL applies to the use of all means and methods of warfare during armed conflict. See ICRC, International humanitarian law and cyber operations during armed conflicts, 2019.

territories.[16] While during the drafting of this rules the inclusion of the prohibition against using propaganda was controversial, the majority voted in favor recognizing that there is a fine line between lawful propaganda and unlawful compulsion.[17]

The second category of IHL rules does not address propaganda or other types of information or psychological operations explicitly; instead, it imposes limits on the effects that can be lawfully pursued by such operations. This category includes a variety of rules, among others the prohibition against encouraging IHL violations,[18] the prohibition of acts or threats of violence the primary purpose of which is to spread terror among the civilian population,[19] the prohibition of orders or threats that no quarter will be given,[20] and the prohibition of ordering the displacement of civilians,[21] including when such encouragements or threats are spread through digital information or psychological operations. IHL also prohibits recruiting children,[22] for example if done through social media. IHL further prohibits exposing prisoners of war to public curiosity[23] as well as all forms of inhumane treatment, outrages against personal dignity, humiliating or degrading treatment against person who do not or no longer participate in hostilities,[24] irrespective of whether traditional or digital means are used. Moreover, during armed conflict perfidy is prohibited[25] and while 'ruse of war' are not prohibited, they have to comply with certain defined conditions, including when relying on information or psychological operations.[26] IHL also requires belligerents to respect

16 Article 51 Fourth Geneva Convention Relative to the Protection of Civilian Persons in Time of War of 12 August 1949.
17 ICRC, Convention (IV) relative to the Protection of Civilian Persons in Time of War. Geneva, 12 August 1949, Commentary of 1958, p. 293.
18 Article 1 common to the Four Geneva Conventions; Rule 139 and 144 ICRC Customary IHL Study.
19 Article 51(2) API; Article 13(2) APII, Rule 2 CIHL Study.
20 Article 23(d) Hague Regulations; Article 40 API; Article 4 APII; Rule 46 ICRC Customary IHL Study.
21 Article 49 GCIV; Article 17 APII; Rule 129 ICRC Customary IHL Study.
22 Article 77(2) API; Article 4(3)(c) APII, Rule 136 ICRC Customary IHL Study.
23 Article 13 GCIII.
24 Article 13 GCIII; Article 3 common to the Four Geneva Conventions; Article 4 APII; Rule 87 ICRC Customary IHL Study.
25 Article 37 API; Rule 65 ICRC Customary IHL Study.
26 Article 37(2) API; Rule 56 ICRC Customary IHL Study.

and protect specific categories of actors, such as medical personnel and humanitarian relief personnel.[27] As will be discussed below, it has also been suggested that information or psychological operations can amount to 'attacks' (as defined in IHL) that would be subject to all IHL principles and rules on the conduct of hostilities. It may further be asked whether they qualify as 'military operations' which must only be directed against military objectives and in the course of which constant care shall be taken to spare the civilian population, civilians and civilian objects.[28]

This paper cannot provide a detailed analysis of all these rules. It will only focus on a select number of IHL obligations that impose limits on digital information or psychological operations.

2.1 Encouragement of IHL violations through information or psychological operations

The prohibition against encouraging IHL violations – irrespective of the means that is employed – derives from a State's obligation to respect and to ensure respect for IHL under article 1 common to the four Geneva Conventions and its customary IHL equivalent, which binds all parties to armed conflicts.[29] This rule requires all parties to armed conflicts to 'ensure respect for international humanitarian law by its armed forces and other persons or groups acting in fact on its instructions, or under its direction or control'.[30] Moreover, in the ICRC's view, it 'would be contradictory if common Article 1 obliged the High Contracting Parties to "respect and to ensure respect" by their own armed forces while allowing them to contribute to violations by other Parties to a conflict'.[31] This view is based on the International Court of Justice's finding that – based on the general principles of IHL – a State party must 'not to encourage persons or groups engaged in the conflict [...] to act in violation of the provisions of

27 See Rules 25, 26, 31, 32 ICRC Customary IHL Study.
28 Article 48 and 58 API; Rule 15 ICRC Customary IHL Study.
29 Article 1 common to the Four Geneva Conventions; Rule 139 and 144 ICRC Customary IHL Study.
30 Rule 139 ICRC Customary IHL Study; ICRC, Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949, Commentary of 2016, paras 143-149. (cited as ICRC Commentary of 2016)
31 Ibid, para. 158. (cited as ICRC Commentary of 2016)

[IHL]'.[32] This finding was made with regard to a manual on 'Psychological Operations in Guerrilla Warfare', which the US provided to a non-State armed group in Nicaragua and which the Court found to encourage IHL violations.[33]

It is widely recognized that this obligation imposes limitations on information or psychological operations: whatever method is applied, no party to an armed conflict may use communication tools – whether offline or online – to 'encourage', 'incite', or 'instigate' IHL violations.[34] It may further be argued that based on States' obligation to ensure respect for IHL, each State has 'a general duty of due diligence to prevent and repress breaches of the Conventions by private persons over which a State exercises authority'.[35] This positive obligation may be interpreted as requiring a State to take active and feasible measures to prevent or halt, for example, digital disinformation or hate speech by private actors within its territory that encourages or incites IHL violations.[36]

While IHL prohibits the encouragement of any IHL violation, the Rome Statute of the International Criminal Court criminalizes acts that order, solicit, or induce the commission of war crimes, i.e. violations of specific IHL rules.[37]

2.2 The use of information or psychological operations to spread certain forms of terror and to cause displacement

IHL imposes limitations on whether and how information or psychological operations – online or offline – may be used to spread fear or terror

32 International Court of Justice, Military and Paramilitary Activities in and against Nicaragua case, Judgment, 1986, para. 220.
33 Ibid, para. 256.
34 See Germany Military Manual, French Military Manual, Canadian Military Manual, United States DoD Manual; New Zealand Defence Force, Manual of Armed Forces Law: Law of Armed Conflict, DM 69 (2 ed.), Volume 4, August 2017, p. 8-40 (cited as New Zealand Military Manual).
35 ICRC Commentary of 2016, para. 150; See also Sassòli, International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare, Edward Elgar Publishing Limited, Cheltenham, 2019, p. 126.
36 An important question in this respect would be how such an obligation relates to States human rights law obligation to respect freedom of expression.
37 Article 25(3) Rome Statute of the International Criminal Court.

among both belligerents and the civilian population.[38] This is explicitly recognized in several military manuals.[39]

With regard to combatants or other persons actively participating in hostilities, IHL prohibits orders or threats that no quarter will be given, including through information or psychological operations.[40] While a commonly proclaimed objective of information or psychological operations is causing defection, mutiny, or rebellion within the armed forces of an adversary,[41] such operations may not threaten that hostilities will be conducted in a way that there shall be no survivors.[42] This long-standing rule of IHL aims not only to prevent IHL violations such as disregarding the obligation to care for the wounded and sick and to protect the life and dignity of detainees but also to prevent 'terrorising the adversary' with such a threat.[43]

IHL further prohibits threats of violence the primary purpose of which is to spread terror among the civilian population,[44] including when issued through information or psychological operations.[45] While there is no doubt that armed conflicts will almost inevitably 'give rise to some degree of terror among the population and sometimes also among the armed forces', this rule prohibits threats of violence that are primarily targeted at spreading terror among civilians.[46] This could, for instance, entail online propaganda or a mass email campaign threatening the annihilation of

38 See footnotes 40, 44, 50 below.
39 See footnotes 42 and 45 below.
40 Article 23(d) Hague Regulations; Article 40 API; article 4 APII; Rule 46 CIHL Study.
41 See, for example, Germany Military Manual; Canadian Military Manual; United States DoD Manual.
42 See, for instance, United States DoD Manual, p. 332.
43 ICRC, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Commentary of 1987, para. 1591. (cited as ICRC Commentary of 1987)
44 Article 51(2) API; Article 13(2) APII, Rule 2 CIHL Study; see also Article 33 GC IV ('all measures of intimidation or of terrorism are prohibited').
45 See Côte d'Ivoire's Teaching Manual, Book III, II.1 on 'Ruses of War', cited here. New Zealand Military Manual, p. 8-40; United States DoD Manual, p. 331-3. Michael N. Schmitt and Liis Vihul (eds), Tallinn Manual 2.0 on International Law Applicable to Cyber Operations, 2nd ed., Cambridge University Press, Cambridge, 2017, para. 6 on Rule 98. (cited as Tallinn Manual 2.0)
46 ICRC Commentary of 1987, para. 1940.

civilian populations.[47] In contrast, experts have concluded that mis- or disinformation that conveys harmful information but does not threaten an attack (this is threaten an act of violence) does not fall under this prohibition.[48] Concretely, this would mean that this rule of IHL may not prohibit, for example, the spread of disinformation 'sent out in order to cause panic, falsely indicating that a highly contagious and deadly disease is spreading rapidly throughout the population',[49] though other rules might prohibit it (see below). In contrast, this rule would prohibit a party to the conflict from threatening that it will use means or methods of warfare to spread such disease among civilians.

It may also be asked whether the IHL rule prescribing that 'parties to a non-international armed conflict may not order the displacement of the civilian population, in whole or in part, for reasons related to the conflict, unless the security of the civilians involved or imperative military reasons so demand', imposes limits on online or offline information or psychological operations.[50] Consider a situation in which a party to an armed conflict spreads disinformation or uses hate speech designed to spread fear among civilians with the objective to displace them. While the wording of relevant IHL provisions seems to limit the prohibition against forced displacement in non-international armed conflict to 'ordering' such displacement, experts have argued – based on the object and purpose of IHL, subsequent State practice and considering the drafting history of Additional Protocol II – that 'ordering in this context is to be construed broadly, interpreted in the sense of a deliberate action on the part of the relevant party'.[51] Otherwise, 'parties would be in a position to avoid their responsibilities by deliberately creating a climate of terror, leaving the civilian population with no other choice but to leave and then claiming that

47 Ibid. See also New Zealand Military Manual, p. 8-40
48 Tallinn Manual 2.0, para. 3 on Rule 98.
49 Ibid.
50 Rule 129 ICRC CIHL Study; article 17 APII.
51 Sivakumaran, The Law of Non-International Armed Conflicts, OUP, Oxford, 2012, pp. 285-286. Sivakumaran flags that the important point is to distinguish such deliberate action from 'voluntary movement on the part of the civilian population'. See also Willms, Without order, anything goes? The prohibition of forced displacement in non-international armed conflict, International Review of the Red Cross, Vol. 91 (875), September 2009, p. 550.

no order was ever given'.[52] Going in a similar direction, the International Criminal Tribunal for the Former Yugoslavia interpreted the crime against humanity of 'forcible displacement' as to include displacement that is caused by 'threats or the use of force, fear of violence, and illegal detention', meaning situations in which 'the displacement takes place under coercion'.[53] As a result, there are strong legal arguments supporting the view that IHL prohibits parties from employing information or psychological operations that threaten or coerce civilians to flee their homes, unless the security of the civilians involved or imperative military reasons so demand.

2.3 Information or psychological operations and IHL principles and rules on the conduct of hostilities

It has further been suggested that in some circumstances, information or psychological operations may amount to attacks as defined in IHL and therefore be subject to the IHL principles and rules on the conduct of hostilities. For instance, the French Military Manual states that if a psychological operation 'amounts to an attack, the means employed are limited and such operations must not be directed against civilians, persons hors de combat, or be perfidious'.[54] Likewise, the Norwegian Military Manual states that certain psychological operations are prohibited, such as 'PSYOPS directed solely or partly at the civilian population that may cause injury or damage to civilians or civilian objects, as such PSYOPS would constitute an attack'.[55]

IHL defines attacks as 'acts of violence against the adversary, whether in offence or in defence'.[56] It is well-established that the notion of 'violence' in this definition can refer to either the means of warfare or their effects, meaning that an operation causing violent effects can be an attack

52 Jacques, Armed Conflict and Displacement: The Protection of Refugees and Displaced Persons under International Humanitarian Law, CUP, Cambridge, 2012, p. 62.
53 ICTY, Prosecutor v. Blagojević & Jokić, Trial Judgement, IT-02-60-T, 17 January 2005, para. 596.
54 French Military Manual p. 68. (translation from French by the author)
55 Norwegian Military Manual, p. 200.
56 Article 49 API.

even if the means used to cause those effects are not violent as such.[57] Accordingly, for the purpose of cyber operations the Tallinn Manual 2.0 defines the notion of 'attack' as 'a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects'.[58] While experts involved in the Tallinn Manual have concluded that 'non-violent operations, such as psychological cyber operations and cyber espionage, do not qualify as attacks',[59] the above-cited military manuals suggest that in some cases information or psychological operations could be expected to cause injury or death to persons or damage or destruction to objects and thus qualify as 'attacks' subject to IHL rules on the conduct of hostilities.

An interpretation of the notion of 'attack' so as to address certain information or psychological (and thereby require that the principles and rules governing attacks apply to these operations) is, however, rather novel and raises several questions. For example, it is unclear whether, and if so how, an information or psychological operation can be said to 'cause' injury, death, or damage. Different scenarios can be envisaged. One scenario could be the incitement of acts which result in injury or death to another person or damage to an object. It is questionable whether such operation can amount to an attack because to cause harm the operation depends on further action by a human that knowingly causes harm to others. Still, such operation will often be unlawful under the prohibition against encouraging or inciting IHL violations (see above). Another scenario could be the deception or misleading of a person into adopting a behavior that the person does not realize as harmful to that person or to others.[60] For this type of operation, it has been observed that 'as opposed

57 See Droege, Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians, 94 IRRC 2012, p. 557; Boothby, The Law of Targeting, OUP, Oxford, 2012, p. 384. As Droege points out, 'it is uncontroversial that the use of biological, chemical, or radiological agents would constitute an attack, even though the attack does not involve physical force'.

58 Tallinn Manual, Rule 92.

59 Tallinn Manual, para. 2 on Rule 92.

60 Geiss and Lahmann provide the example of disinformation spread by State A among soldiers (and eventually civilians) of State B about inhaling methanol to combat a respiratory disease, which is designed to, and actually causes, death among the addressees. Geis and Lahmann, Protecting the Global Information Space in Times of Armed Conflict, 2021, p. 4; available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3784565.

to a cyber operation against an IT system that triggers a physical chain of events that leads to damage, an instance of disinformation requires the targeted audience to act upon the received information and because of that inflict harm on itself'.[61] However, at least when the intent and effect of an information or psychological operation are similar to a kinetic attack (i.e. injury, death, damage) and only the method to deliver the effect is different (in this case deceiving the targets into adopting a behavior that they are unaware will actually harm themselves or others), it could be queried whether such difference should have any relevance under IHL. For instance, the Norwegian Manual considers that: 'An [...] unlawful PSYOPS is distributing information with the aim of misleading civilians to cause them injury.'[62]

Furthermore, opinions diverge on whether information or psychological operations could fall under the broader notion of 'military operations', which may only be directed against military target,[63] and in the conduct of which 'constant care shall be taken to spare the civilian population, civilians and civilian objects'.[64]

In sum, when a psychological or information operation could qualify as an attack or as a military operation remains to be further studied.

2.4 Information or psychological operations against specifically protected actors

For humanitarian and medical actors, online misinformation, disinformation and hate speech are a growing concern. In practice, misinformation that undermines their acceptance and work – or causes objection and violence against them – may unfold 'organically',

61 Ibid, p. 17. One suggestion for a legal test to establish a sufficiently strong link between an information or psychological operation and human or physical harm could be the standards developed in international criminal jurisprudence for 'inciting' or 'inducing' international crimes.
62 Norwegian Military Manual, p. 200.
63 Article 48 API.
64 Article 57 API; Rule 16 ICRC Customary IHL Study. For a discussion of the notion of 'military operation', see, for example, Droege, Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians, p. 556; Geis and Lahmann, Protecting the Global Information Space in Times of Armed Conflict, p. 15-16.

for instance as the result of a misunderstanding or dissatisfaction with services. In other cases, however, humanitarian or medical personnel have become the target of disinformation or intentionally defamatory social media campaigns, which can result in threats or attacks against them.[65]

While IHL protects medical and humanitarian personnel and facilities as civilians and civilian objects, it also provides additional special protection for these actors.

Regarding medical personnel, IHL requires that belligerents to respect and protect medical facilities and personnel at all times.[66] The obligation to 'respect' medical facilities and personnel is understood as a prohibition not only against attacking but also against 'harm[ing] them in any way. This means that there should be no interference with their work (for example, by preventing supplies from getting through) or preventing the possibility of continuing to give treatment to the wounded and sick who are in their care'.[67] The obligation to 'protect' medical personnel and facilities also entails positive steps, namely an obligation to actively take measures to protect them against harm to the extent feasible.[68] Applied to information or psychological operations, this suggests that conducting such operations with the objective to harm medical services or to disrupt their work is

65 See ICRC, Harmful Information: Misinformation, Disinformation and Hate Speech (MDH) in Conflict and Other Situations of Violence, forthcoming.

66 See, for instance, Art. 19 GCI; Art. 12 GCII; Art. 18 GCIV; Art. 12 AP I; Art. 11 APII; Rules 25, 28, 29 ICRC Customary IHL Study; Tallinn Manual 2.0, Rules 131-132. Protection of medical facility and personnel ceases only if they commit, or are used to commit, outside their humanitarian duties, acts harmful to the enemy. Protection may, however, cease only after a due warning has been given, naming, in all appropriate cases, a reasonable time limit and after such warning has remained unheeded. See Art. 21 GC I, Art. 34 GC II; Art. 19 GC IV; Art. 13 AP I; Art. 11(2) AP II; Rules 25, 28, 29 ICRC Customary IHL Study; Tallinn Manual 2.0, Rule 134.

67 ICRC commentary of 1987, para. 517. See also ICRC commentary of 2016, para. 1799. See also The Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector, May 2020: "5. During armed conflict, international humanitarian law requires that medical units, transport and personnel must be respected and protected at all times. Accordingly, parties to armed conflicts: must not disrupt the functioning of health-care facilities through cyber operations; must take all feasible precautions to avoid incidental harm caused by cyber operations, and; must take all feasible measures to facilitate the functioning of health-care facilities and to prevent their being harmed, including by cyber operations." available at: https://www.elac.ox.ac.uk/the-oxford-Statement-on-the-internation-al-law-protections-against-cyber-operations-targeting-the-hea; Tallinn Manual 2.0, para. 5 on Rule 131.

68 ICRC Commentary of 2016, para 1805-1808; Tallinn Manual 2.0, para. 6 on Rule 131.

prohibited. It furthermore suggests that parties to the conflict must take active and feasible measures to prevent or halt, for example, disinformation or hate speech against medical personnel or facilities by actors under their control.

IHL also prescribes that humanitarian personnel and relief consignments must be respected and protected.[69] In analogy to the obligation to respect and protect medical personnel and facilities, the relevant rules should also be understood as prohibiting attacks against humanitarians as well as 'other forms of harmful conduct outside the conduct of hostilities' targeted at humanitarians or that unduly interfere with their work.[70] Moreover, parties to armed conflicts are required to agree, allow and facilitate humanitarian relief operations.[71] Thus, information or psychological operations that aim to incite violence against humanitarian personnel or relief consignments are prohibited. Moreover, operations that aim to interfere with their work are unlawful, for instance operations that instigate protest to block roads and hinder humanitarians from reaching affected populations. In fact, parties to armed conflicts have an obligation to take feasible measures to prevent or halt such operations, for example if lead by private actors.

3. Conclusion

As new and digital technologies are prevalent in environments affected by armed conflicts and used by belligerents to achieve their objectives, there is a risk that certain forms of information or psychological operations are also employed to cause serious humanitarian consequences, such as violence against civilians, displacement, or the hindering of medical and humanitarian services. There is general agreement that many forms of information or psychological operations – online or offline – are either

69 Articles 70(4) and 71(2) of AP I; Rule 31 and 32 ICRC's Customary IHL Study.
70 ICRC Commentary of 2016, paras 1358 and 1799. Along the same lines, the group of experts that prepared the Tallinn Manual 2.0 identified an IHL rule requiring: 'Cyber operations shall not be designed or conducted to interfere unduly with impartial efforts to provide humanitarian assistance' (Rule 145). Such cyber operations are prohibited 'even if they do not rise to the level of an "attack"' (para. 4 of the commentary on Rule 80).
71 See, for instance, article 59 GC IV and article 69–70 AP I, Rule 55 of the ICRC's Customary IHL Study.

not regulated by or not in violation of IHL. Yet, it would be wrong to infer that the use of online information or psychological operations during armed conflict is unconstrained by law. While only very few rules of IHL address such operations explicitly, there are several rules that impose important limits, for instance by prohibiting the encouragement of IHL violations, by prohibiting certain forms of operations that impose fear and terror, or by providing specific protection for medical and humanitarian actors. Further analysis is needed, however, on several questions, including whether (and if so, under what circumstances) information or psychological operations can qualify as 'attacks' or military 'operations' and thus be subject to IHL rules on the conduct of hostilities.

This paper could only examine some of the relevant IHL rules; additional IHL rules are relevant as well. Moreover, to adequately assess the lawfulness of digital information and psychological operations during armed conflict, other bodies of international law have to be considered alongside IHL.

6 The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Ransomware Operations

Published 4 October 2021
122 Signatories

Reiterating the commitment expressed in the First, Second, Third and Fourth Oxford Statements to clarify rules of international law applicable in the use of information and communications technologies;

Noting that ransomware (i.e. malware designed to encrypt data and render it unavailable unless a demand is met) is a global threat, having been employed at an escalating pace by a growing number of malicious actors, including states and non-state groups for financial or political purposes, often connected to criminal and other unlawful activities such as terrorism, human and drug trafficking, money laundering, sanctions evasion, and the proliferation of weapons of mass destruction;

Stressing that the COVID-19 pandemic and our increased dependency on the Internet and other information and communications technologies have enhanced vulnerabilities to and opportunities for ransomware and other types of malware that facilitate its distribution, including the targeting of remote control or monitoring systems and the use of phishing emails, malicious websites or false notifications;

Considering that ransomware has, in the vast majority of cases where it has been employed, caused significant and widespread harm to public and private institutions, as well as individuals, such as financial loss, reputational damage, breach of confidentiality, and the significant disruption of critical infrastructure, including healthcare and education, while posing an imminent risk of destructive harm to industrial control systems such as electric grids, water distribution systems and nuclear power plants;

Bearing in mind that ransomware can take increasingly varied and sophisticated forms, including targeted and indiscriminate operations, and lead to the denial of access to and/or the unauthorized release of data if demands are not met;

We agree that:

1. Conduct carried out through information and communications technologies, such as ransomware operations, is regulated by international law.

2. States must refrain from conducting, directing, authorising or aiding and assisting ransomware operations which violate the principles of sovereignty or non-intervention in a state's internal or external affairs, or amount to a prohibited threat or use of force within the meaning of the Charter of the United Nations. In particular, states must refrain from ransomware operations which are aimed at or result in disruption to electoral systems, healthcare, electric grids, water distribution systems, and nuclear power plants.

3. States must refrain from conducting, directing, authorising or aiding and assisting ransomware operations that result in violations of the human rights of individuals within their jurisdiction, such as the right to life, health, private life, education, property, freedoms of thought and opinion, freedom of expression, including the freedom to seek, receive and impart information and ideas of all kinds.

4. a) States must not allow their territory or infrastructure under their jurisdiction or control to be used by states or non-state actors for ransomware operations that are contrary to the rights of other states, when the former states know or should know of such operations.

b) To discharge those duties, states from which ransomware operation emanates, in full or in part, must take feasible measures to stop such operations and otherwise address the situation. Such measures may include the conduct of investigations, the adoption of legal and technical measures, as well as cooperation with other states. Any measures taken in this regard must be compliant with applicable obligations under international law, including international human rights law.

5. States must take measures to protect the human rights of individuals within their jurisdiction from harmful ransomware operations, including when such operations are carried out by other states and non-state actors. To discharge this obligation, states may, among other measures, prohibit ransomware by law, take feasible steps to stop ransomware operations,

mitigate their effects, investigate and punish those responsible, as well as prevent and suppress ransom payments to the extent possible. Where such protective measures interfere with other human rights, they must conform with applicable legal requirements, such as legitimate purpose, legality, necessity, proportionality and non-discrimination.

6. The use of ransomware during armed conflict is subject to the applicable rules of international humanitarian law (IHL). These rules include, but are not limited to, the duty to respect and ensure respect for IHL, which entails an obligation to prevent violations of IHL; the duties to respect and to protect specific actors or objects, including medical personnel and facilities and humanitarian personnel and consignments; the duties concerning objects indispensable to the survival of the civilian population as well as those concerning works and installations containing dangerous forces; and other rules on the protection of civilians, civilian objects, and of persons who no longer participate in hostilities, such as the sick, wounded, and prisoners of war.

7. The use of ransomware will amount to international crimes, such as genocide, war crimes and crimes against humanity, where the elements of those crimes are fulfilled.

8. The application of the aforementioned rules is without prejudice to any other applicable rules of international law that provide protections against ransomware and related activities.

The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Ransomware Operations

Written by Dapo Akande, Antonio Coco, Talita de Souza Dias, Duncan Hollis, James O'Brien and Tsvetelina van Benthem

First published on EJIL:Talk!, Just Security and Opinio Juris

In the past few months, nothing has reminded everyone of the etymology of the expression 'computer virus' like ransomware. This form of malicious code is delivered through a vulnerability in the victim's system, such as a phishing email or password spraying, infiltrating and potentially crippling it like a disease. Specifically, ransomware is used to encrypt user data and either delete or release that data unless a demand (commonly for money) is met. Ipso facto, ransomware causes by definition adverse consequences for its intended and unintended targets. Even when the ransom is paid or the attacker's demand is eventually met, frequently a portion of the encrypted data will have been lost anyway and the victim may be forced to stay offline for a while, incurring significant costs to repair or change its systems.

Where the victim serves others, for example, providing public goods like healthcare, education, or utilities, the adverse consequences can quickly, and foreseeably, spread beyond the ransomware's initial targets. In other cases, the means by which ransomware is delivered — especially when delivered through or as part of a digital supply chain attack — can produce a range of cascade effects harming entities who were not the "real" target of the operation but nonetheless suffer its consequences. Recent months saw a significant surge in ransomware operations. For instance, in May 2021, Colonial Pipeline, a United States oil pipeline

system carrying gasoline and jet fuel, was forced to halt its operations to ensure system safety following a ransomware attack. As a result, there was panic buying and shortage of gasoline which led to the highest average gasoline prices in the US for seven years. The attack on the meat provider JBS has been connected to a rise in the price of beef and pork. In the United Kingdom, ransomware attacks have targeted the education sector with increasing frequency, leading to the loss of student coursework, school financial records and data relating to COVID-19 testing. The internal network of Brazil's National Treasury was hit by ransomware in August 2021, and September saw a ransomware operation against South Africa's Justice Department. It is no wonder that — using an expression that has sadly become all too common — we are witnessing a 'ransomware epidemic'. The cost of this epidemic, both financially and otherwise, may be very high. According to recent reports, India saw a significant increase in the financial impact of ransomware operations: the approximate recovery cost from the impact of ransomware tripled in the last year, up from $1.1 million in 2020, to $3.38 in 2021.

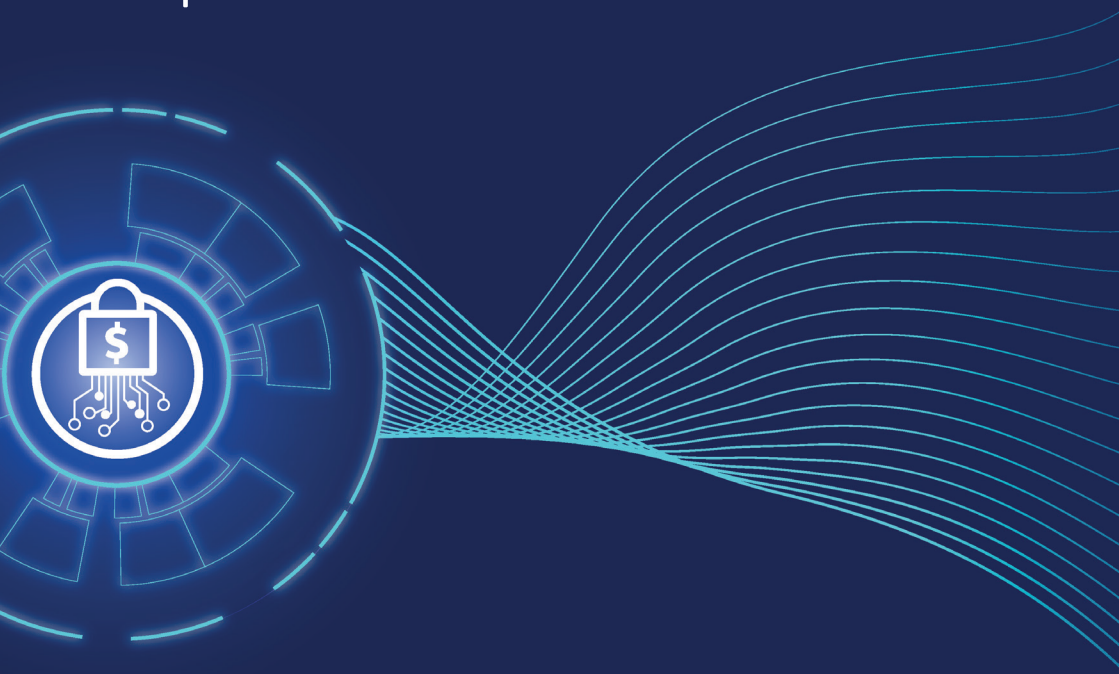
The ever-growing number of attacks and increased professionalisation of actors behind ransomware operations call for robust action by states to meaningfully protect cyber infrastructure under their jurisdiction and control. Countering ransomware is not just a matter of national security and good governance. It is an obligation under international law, one highlighted in the latest, and fifth, Oxford Statement on the Protections of International Law in cyberspace. Like previous iterations of the Oxford Process, the Fifth Statement aims to reflect existing principles and rules of international law in their application to cyber operations and to call upon all states and other international actors to abide by them. Previous Oxford Statements on international law protections in cyberspace have focussed on the rules of international law when viewed from the perspective of objects or processes which deserve protection, e.g. the rules which apply to cyber operations that target the health sector, vaccine research, electoral processes. However, as

with our Fourth Statement, which sets out rules relating to information operations and activities, the present Statement focuses on a specific type or method of cyber operation.

While it may appear obvious that states must not themselves engage in ransomware, calling into play a set of negative obligations under international law, this is just the starting point. Ransomware is a problem not only when state-directed or state-sponsored, but even when carried out by non-state actors and tolerated or acquiesced in by different states, including the one from which it originates. For this reason, all states have an obligation to give effect to the well-established rules of international law requiring them to adopt protective measures against the harm caused by ransomware operations which are carried out by others. Those impose obligations not only to take feasible measures to put an end to harm caused to the rights of other states but also to take measures to prevent the infringement of the human rights of persons within the state in question. Duties to protect against ransomware may be complied with in several ways, ranging from the investigation and punishment of those responsible for ransomware and the training of specialized cybersecurity personnel, to the adoption of technical measures to strengthen cyber infrastructure, international cooperation and information-sharing. We very much hope that the adoption of these and other measures against ransomware will constitute an effective remedy, if not a cure against the particularly pernicious form of cyber operation that ransomware embodies.

Our survey of existing international law — whose results are enshrined in the Statement reproduced below — reveals that there is no space for ransomware in a healthy, peaceful, and prosperous international community. All states are called upon to fully commit to this vision.

Virtual workshop
Report



The Oxford Process on International Law Protections in Cyberspace:

The Regulation of Ransomware Operations

20 July 2021

Executive Summary & Key Takeaways

On July 20th, 2021, the Oxford Institute for Ethics, Law and Armed Conflict (ELAC) held a virtual workshop, sponsored by Microsoft, on the regulation of ransomware operations under international law. This workshop was part of the Oxford Process on International Law Protections in Cyberspace, an initiative seeking to identify areas of consensus on international legal rules in their application to cyber operations impacting specific objects or employing certain means or methods. This workshop was the sixth in the Oxford Process series, following workshops on the protection of the healthcare sector (May and July 2020), electoral processes (October 2020), IT supply chains (March 2021) and the regulation of information operations (April 2021).

Insidious and coercive, ransomware operations have become one of the scourges of the 21st-century digital landscape. Beyond causing extensive economic harm, such operations have disrupted the functioning of critical infrastructure and social services across jurisdictions. No continent has been spared from the threat of ransomware. Against this background, the sixth Oxford Process workshop sought to identify the contours of the applicable international legal rules that regulate ransomware operations. The following points emerged from the discussion:

1. International law applies to ransomware operations and is indeed a relevant and crucial framework for addressing the risks inherent in such operations.

2. Ransomware operations are operations that deploy malware designed to encrypt data and render it unavailable unless a demand is met.

3. International law regulates ransomware operations through a complex system of rules that protect both State and individual interests. Additional work is needed on the specification of rules, and specifically on elements of scale and effects (for the prohibition of the use of force and the rule of sovereignty), coercion (for the rule of non-intervention), transboundary harm (for the no-harm principle).

4. An emphasis should be placed on the positive obligations of States in relation to ransomware operations. One of the main conditions that allowed the proliferation of ransomware operations is the weakness of cyber defence systems, including those of entities operating critical infrastructure networks. Thus, under a range of legal frameworks, including international human rights law, States must provide an adequate domestic legal framework for combating ransomware, take all necessary steps to prevent, mitigate and redress the harm of ransomware operations, investigate incidents and, where appropriate, extradite or prosecute perpetrators.

5. While States and other stakeholders must work together to specify the contours of obligations under general international law, the time may be ripe for creative thinking on other international instruments that may be relevant to the protection against ransomware.

Background

Recent years saw a significant surge in ransomware cyber operations. In May 2021, Colonial Pipeline, a United States oil pipeline system carrying gasoline and jet fuel, was forced to halt its operations to ensure system safety following a ransomware attack. In the United Kingdom, ransomware attacks target the education sector with increasing frequency, and have already led to loss of student coursework, school financial records and data relating to Covid-19 testing.

As the threat rises, so does the understanding of States that robust

actions are needed to meaningfully protect cyber infrastructure. For instance, on June 9th, 2021, the US Cybersecurity and Infrastructure Security Agency published Rising Ransomware Threat to Operational Technology Assets, a fact sheet including several recommended actions and resources that critical infrastructure entities should implement to reduce the risk of the ransomware threat. And on June 14th, Lindy Cameron, chief executive of the National Cyber Security Centre, stated that ransomware is the biggest threat to online security for individuals and businesses in the United Kingdom. She also warned that ransomware operations are becoming increasingly professionalised.
Unlike the first four Oxford Process workshops which focused on a set of objects of protection, this workshop examined the regulation of a particular type of cyber operation. Through its three substantive sessions, the workshop analysed the regulation of ransomware from the perspective of both negative and positive obligations under international law.

Summary of Sessions

Welcome and Introduction

Professor Dapo Akande (ELAC) gave the introductory remarks, welcoming the workshop participants to the sixth event of the Oxford Process series. Established in May 2020, the Oxford Process is an initiative seeking to identify areas of consensus on the ways international law applies to cyber operations. While the first four events of the Oxford Process focused on the international legal protection of particular objects, namely the healthcare sector, electoral processes and IT supply chains, the fifth and sixth ones transitioned to the regulation of particular techniques employed by cyber operations – information operations and ransomware. For this workshop on ransomware, the objective was to explore the scope of the relevant international legal rules in their application to this specific type of activity.

The workshop was organised into three sessions. The first session, A Landscape of Ransomware Threats, was aimed at providing the

participants with the technical state of play of ransomware operations. The second session explored legal duties to refrain, that is, negative obligations under international law, while the third focused on positive obligations, obligations to take certain measures to protect against ransomware operations. Each session was composed of two presentations followed by an open roundtable discussion.

Session I

A Landscape of Ransomware Threats

Chris Krebs, Partner, Krebs Stamos Group LLC

Mr Krebs offered a reflection on the conditions that allow the proliferation of ransomware operations and the ways to address that proliferation.

It was noted that the scourge of ransomware in Western democracies has been on the radar of cybersecurity experts for more than a decade, even though 2020 and 2021 made that threat more visible to the public due to a number of large-scale and widely documented ransomware operations.

For ransomware operations to spread as they have, they need the right conditions. Mr Krebs identified an 'unholy trinity' of conditions that allow that spread: first, poor defences across critical infrastructure and the private sector; second, the emergence of cryptocurrencies; and third, fertile ground in host nations for ransomware groups to operate with impunity.

On the question of how to address the rising threat of ransomware, it was suggested that the responses largely map onto the conditions. States must continue to improve their cyber defences at home. For instance, a growing understanding of the importance of cyber security for critical infrastructure in the United States led to a governmental approach emphasizing security uplifting through federal requirements and the issuance of directives to improve security in particular

sectors, such as the pipeline sector. This approach aims to set minimum cybersecurity standards. Another piece of the puzzle is the regulation of cryptocurrency markets, which requires additional insights into the interaction between crypto and the traditional cash economy. And finally, a robust response to ransomware would necessitate the dismantling of ransomware groups, a response that must include transnational cooperation and potentially a ramping up of sanctions regimes.

Ciaran Martin, Professor of Practice in the Management of Public Organisations, Blavatnik School of Government, University of Oxford

Building on the previous presentation, Professor Martin provided an overview of existing ransomware risks, the evolution of ransomware operations and the response options available to States.

Part of the reason for the increased amount of attention paid to ransomware operations is that the harms produced have become much worse over the years and have, in many ways, confirmed the worst prognoses of what cyber harms may look like. The closest human beings have come to being physically hurt as a consequence of cyber operations has been through the actions of avaricious cyber criminals without a political agenda. Ransomware has, in recent years, caused significant societal disruption by directing operations against the education sector and even targeting the entire national healthcare system of the Republic of Ireland. From activities concentrated on the secret extortion of rich companies, ransomware operations have now come to directly and indirectly impact all sectors of human life.

Professor Martin guided the participants through a few evolutions observed in ransomware operations: from network intrusions where the victim is locked out of its system until the demand is met (what could be termed classic ransomware) through operations that threaten to leak data online to ransomware that attacks the supply chain, thus impacting a core supplier rather than going after individual users.

In considering the way forward, Professor Martin emphasised the need to think carefully about the legal duties of entities hosting critical networks, as well as the problem of under-implementation and under-enforcement of international obligations. It was suggested that inspiration could be drawn from other regimes that have achieved some success in curbing harmful behaviour, such as that of terrorism financing following the 9/11 attacks. Finally, it was noted that while a growing number of States consider the reckless endangerment of critical infrastructure through ransomware a national security risk, there continues to be a mismatch between this latter qualification and the reality of privatised responses to the ransomware threat.

Open discussion

In the open discussion, the participants considered the interaction between the regulation of cryptocurrencies and the curbing of ransomware operations. One participant inquired into the options for freezing a particular cryptocurrency and reimbursing its lawful users. Another participant considered that a focus on the kill chain of cryptocurrency payments may be misplaced. At minimum, it was agreed that the crypto economy needs to be more transparent. It was suggested that minimum mandatory reporting of breaches on the part of victims may assist governments in responding swiftly and adequately to the threat.

Session II

Ransomware Operations and Negative Obligations under International Law

Moderated by Professor Duncan Hollis, Temple Law School

At the beginning of the session, the moderator asked the participants to consider the ways in which ransomware operations may challenge presumptions that operate in the sphere of cyber operations. For instance, while in the past the attacking of particular targets, such as power grids, may have been taken as a strong indicator that an attack had been mounted by a nation State actor, the contemporary landscape

of ransomware operations shows that such operations can be launched by non-State actors operating without any political motivation.

Liis Vihul, Chief Executive Officer, Cyber Law International

The presentation offered a reflection on a number of negative obligations under international law, namely the prohibition of the use of force and the rules of sovereignty and non-intervention. Duties to refrain under international human rights law were not considered in detail except as a reminder that the issue of the extraterritorial application of human rights treaties continues to loom large, and that any discussion on human rights would be highly dependent on the specifics of particular ransomware operations, and in particular on how they affect the enjoyment of rights.

For the obligations considered by Ms Vihul, a first necessary condition is to establish attribution to a State. The reality of ransomware operations, however, demonstrates that most of these operations are conducted by non-State actors that do not evince the types of connections necessary under the attribution thresholds of general international law. Thus, the majority of ransomware operations are best dealt with under domestic law and the cybercrime ecosystem. For those ransomware groups that do have connections to State actors, it was highlighted that while the test of conduct 'directed, instructed or controlled by a State' remains the most likely ground for attribution, international lawyers should also look beyond it to other grounds of attribution, as outlined in the Articles on State Responsibility.

Turning to the substance of the rules, Ms Vihul began her analysis with the prohibition of the use of force. The main difficulty for the application of this prohibition is the identification of the threshold of 'force', and, relatedly, the threshold of 'armed attack' as a trigger for the right to self-defence under Art. 51 of the Charter of the United Nations. While there seems to be widespread agreement on the 'scale and effects' test developed in the jurisprudence of the International Court of Justice,

how one is to ascertain the relevant scale and effects remains the more complex inquiry. Usually, 'effects' are conceptualised on a spectrum with non-consensual physical effects on one end and merely negligible negative effects on the other, while 'scale' is understood as referring to the quantum of said effects. An example of negative effects between the two ends of the spectrum would be a ransomware cyber operation that deletes or locks data and as a result causes functional, as opposed to physical structural, damage.

On sovereignty, Ms Vihul acknowledged the continuing debate on the 'sovereignty as a principle' and 'sovereignty as a rule' approaches. On the assumption that sovereignty is indeed a self-standing rule, its substance is widely understood to cover territorial integrity and inviolability (by prohibiting causing certain effects on the territory of the target state), on the one hand, and interference with inherently governmental functions, on the other. An issue that ransomware operations raise particularly acutely is that of the nature of harms covered by the rule.

While some ransomware operations manifest effects that combine economic harms and other types of damage (the Colonial Pipeline being an apposite example, with its physical effects on the ground through gas shortages and system disruption), most cause purely economic effects.

A crucial question is whether economic harms ought to be taken into account when assessing ransomware operations for the purposes of the sovereignty rule. Just as economic pressure was not included within the meaning of 'force' for the purposes of the use of force prohibition in the Charter of the United Nations, sovereignty has traditionally focused on the protection of territorial integrity rather than safeguarding against economic harms. That said, some States seem to be moving in the direction of accepting that cyber operations causing significant financial harm may be wrongful under international law. The question thus remains unsettled.

Another crucial discussion is that of the unintended and unconstrained effects of ransomware. For instance, many consider WannaCry as a cyber operation gone wrong. Two specific issues arise: one on intent and a second on causality. On intent, the question is whether it is a constitutive element of the relevant international legal rules. This is an unsettled issue. On causality, the question is whether and, if so, to what extent one must account for the downstream effects of an operation. This question was illustrated through the JBS meat producer plant ransomware attack, where the meat supplier had to halt operations, which then reportedly upended the daily life of employees. The downstream effects of ransomware operations can be very far-reaching, which makes the drawing of lines particularly important. Additional questions arise when the harmful effects are co-produced by the ransomware operation and the actions of the victim, for instance where a ransomware operation targets a bank, which pays the ransom, and subsequently suspends operations for two weeks in order to conduct internal audits – do the qualifying effects extend to the harm caused through these two weeks of the interruption of activities?

On non-intervention, Ms Vihul noted that there is agreement on the two elements of the rule – an interference in the *domaine réservé* of a State and the coercive nature of the interference. However, the main question revolves around the notion of coercion. While ransomware is by definition coercive in the everyday meaning of the term, it may fall short of the notion of coercion for the purposes of the non-intervention principle. This is because ransomware operations may not seek to coerce a State to do something, even though they may effectively place it in a position it would not have been in but for the operation. WannaCry was considered a good illustration of the problem. While North Korea did seek to coerce the payment of money, it did not intend to coerce the United Kingdom with regard to its health policy.

A final note was made on response options and the boundaries of enforcement jurisdiction. It was noted that more work is needed on

identifying the legal qualification of enforcement acts of hacking into perpetrator systems located outside the State's territorial jurisdiction. This discussion would also require an investigation into the applicable circumstances precluding wrongfulness under general international law.

Asaf Lubin, Associate Professor of Law, Indiana University Maurer School of Law

In this presentation, Dr Lubin sought to, first, expand the conversation on how to internationalise the crime of ransomware and, second, widen the pool of sources for deriving negative and positive obligations related to ransomware. The presentation followed three steps: (1) a description of how ransom is dealt with in domestic criminal law; (2) the consideration of ransomware as an international crime; (3) an overview of the implications of the proposed internationalisation.

On the domestic regulation of ransomware, Dr Lubin noted the heterogeneity of regulation across jurisdictions. In the United States, multiple States have already legislated on ransomware as a specific crime, criminalising the possession and distribution of the malware, as well as the use of ransomware to commit computer extortions. However, the regulation is not uniform in the way the crime is defined. Other countries have yet to adopt ransomware-specific statutes and thus rely on their general statutes to deal with the rising threat, including through the cyber offences of 'unauthorised access to computer networks' and the general crime of 'extortion.' No jurisdiction has criminalised negotiations with ransom groups and only a handful of States have criminalized or deterred through other means the payment of ransom. For now, domestic legislation is patchy, scattered and non-comprehensive.

On the consideration of ransomware as an international crime, Dr Lubin suggested looking into the literature on the evolution of international crimes from piracy through hostage-taking to human trafficking and terrorism. Considering the perpetrator of ransomware as a *hostis humani*

generis (enemy of mankind) would, according to Dr Lubin, provide a wider menu of options for countering the threat of ransomware. Public regulation of ransomware was seen as a way to centralise international efforts, including enforcement action. While it was acknowledged that the likelihood of new international instruments specifically regulating ransomware is low, Dr Lubin suggested opting for an interpretation of existing treaties, such as the 1979 International Convention against the Taking of Hostages, that would cover certain categories of ransomware operations. For instance, the definition of the offence of hostage-taking in the Convention provides that 'any person who seizes or detains and threatens to kill, to injure or to continue to detain another person in order to compel a third party, namely a State, an international intergovernmental organisation, a natural or juridical person, or a group of persons, to do or abstain from doing any act as an explicit or implicit condition for the release of the hostage'. According to Dr Lubin, this text can potentially apply to particular recent instances of ransomware operations targeting hospitals, where patients were 'seized' in the course of the attack.

On implications, it was noted that the internationalisation of the crime of ransomware would create a baseline of illegality, provide the international community with a range of specific obligations that are better tailored to the crime, and open doors for the operationalisation of responsibility by allowing recourse to the International Court of Justice and establishing a basis for universal jurisdiction. Dr Lubin's full analysis is summarised in The Law and Politics of Ransomware, forthcoming in a special symposium issue of the Vanderbilt Journal of Transnational Law.

Open Discussion

The discussion revolved around four main themes – the definition of ransomware, attribution, ransomware as an international crime, and due diligence.

Starting with the definition of ransomware, some participants questioned the focus on monetary payment as a constitutive element of the offence. Rather, agreement seemed to coalesce over a position that the demand of the perpetrators can take a variety of forms and need not be economic in nature.

On attribution, a number of participants considered the distinction between purely private acts of State organs and entities exercising elements of governmental authority (that would not be attributable to a State) and acts ultra vires (that would be attributable). In particular, participants discussed the relevance of the use of office buildings, tools and techniques in the conduct of ransomware operations, even if such operations are not launched as part of a person's official functions or during office hours.

On the turn to considering ransomware perpetrators as *hostis humani generis*, some participants expressed concerns that this move would fail to capture State conduct. This concern was then countered by pointing to the reality of ransomware operations: most ransomware attacks are not performed by States. Another concern was that, if States are unwilling to regulate ransomware specifically at the international level, expanding the interpretation of existing instruments may be met with similar resistance.

On due diligence, one participant noted the importance of duties of States to ensure that their territory or areas under their jurisdiction are not used for the commission of internationally wrongful acts. A reason for the significance of this duty in the context of ransomware is the rampant inactivity of host States from which criminal ransom groups operate.

Session III

Ransomware Operations and Positive Obligations under International Law

Moderated by Dr Talita Dias, ELAC

In this session, the speakers were asked to address positive obligations under international law, prompted by four hypothetical scenarios (addendum 1).

Rebecca Crootof, Assistant Professor of Law, University of Richmond School of Law

Professor Crootof considered the positive obligations arising in the context of ransomware in a chronological order. Some positive obligations arise before the ransomware operation – an example here are obligations to criminalise ransomware in domestic legal systems. Others are triggered by the operation, and thus arise during the ransomware operation. These obligations include duties to make every reasonable effort to halt and mitigate the harm of ransomware. It was queried whether one way of discharging such positive obligations could take the form of a request for assistance. Finally, States are bound by positive obligations after the ransomware operation – examples are the duties to investigate, extradite or prosecute perpetrators.

It was further suggested that, for a possible Oxford Statement on the regulation of ransomware, the drafters ought to formulate a robust set of due diligence obligations, while at the same time remaining mindful that such a robust formulation should not incentivise State monitoring that contravenes human rights or would prompt escalatory responses, such as countermeasures. Professor Crootof noted her concern over the increased recourse to self-help in the international community.

In a final note on the way forward, Professor Crootof suggested focusing more attention on due diligence as a standard of liability when implementing a duty to compensate. One of the main benefits of understanding due diligence as a standard of liability, according to the speaker, is that it provides another non-escalatory option for States

in the toolbox of measures for addressing the harm of ransomware. Importantly, it would also increase the chances that ransomware victims would receive compensation.

Joanna Kulesza, Professor of Law, University of Lodz

In her remarks, Professor Kulesza focused on three main issues: terminology, due diligence, and the importance of engaging with both State and non-State actors on the threat of ransomware.
Starting with terminology, Professor Kulesza raised the question of the definition of 'cyber infrastructure', noting that more clarity may be needed on the boundaries of this phrase. She also noted some international efforts to broaden the objects of protection, for instance, The Netherland's proposal to specifically protect the public core of the internet.

Turning to due diligence, Professor Kulesza emphasised the importance of considering both the Corfu Channel rule and the no-harm principle within the confines of a possible Oxford Statement on ransomware. In particular, it was noted that the Corfu Channel rule would be satisfied by the presence of not only actual, but also constructive knowledge. It was emphasised that due diligence obligations, which trigger specific duties, such as the conduct of risk assessments and the establishment of a well-functioning law enforcement system and legal framework, have the capacity to ensure a good governance standard across jurisdictions. On the no-harm rule, Professor Kulesza, while agreeing that the harms covered can be wide-ranging in nature, cautioned about possible resistance from some Sates to the consideration of harms beyond the environmental realm within the ambit of the rule. She also urged the participants to look for inspiration in the Budapest Convention, which contains a range of concrete positive duties. The Budapest Convention was also raised as a good example of a technology-neutral instrument that can have spill-over effects for the bolstering of protections even for States that are not parties (for instance, such a spill-over was illustrated through the intersection of the Budapest Convention and the European

Union General Data Protection Regulation).

Finally, Professor Kulesza noted that cooperation on countering the threat of ransomware needs to extend beyond academia and State actors to non-State actors working in the area. For instance, it was noted that a number of corporate actors are active in the Domain Name System abuse space.

Open discussion

The open discussion centred on two main questions: a possible obligation not to pay ransom and the scope of the no-harm rule. On a possible obligation not to pay ransom, participants seemed to coalesce that any blanket criminalisation would be arbitrary and harmful. The reality of ransomware operations shows that the harms at stake may be human life and health, for instance in operations against hospitals. One participant opined that a viable alternative may be the crafting of a general prohibition with a framework of exceptions.

On the scope of the no-harm rule, one participant expressed a concern that an expansive view of 'transboundary harm' may swallow the rest of international law. This is because, if such harm is not confined in some meaningful way, it would include economic, political, social or any other type of harm which may be the subject of other specific rules of international law, such as the prohibition on the use of force. While other participants adopted a broad approach to the types of harms at stake, considering that the rule extends beyond environmental and otherwise physical harms, they noted that the necessary limitations on the rule can come through the qualifier of 'significant' harm, standards of causation, knowledge and liability. Support for this broader conception of harm was rooted in the work of the International Law Commission.

List of Workshop Participants

1) Christiane Ahlborn, Legal Officer, UN Office of Legal Affairs
2) Dapo Akande, Professor of Public International Law and Co-Director, Oxford Institute for Ethics, Law & Armed Conflict (ELAC), University of Oxford
3) Leonie Arendt, Policy Consultant, UN Foundation
4) Stephany Aw, Deputy Senior State Counsel, International Affairs Division, Attorney-General's Chambers of Singapore
5) Sandra Birrer, Lawyer, Federal Department of Foreign Affairs FDFA, Directorate of International Law, International Law Division, Switzerland
6) Brishailah Brown, Microsoft
7) Scott Charney, Vice President, Security Policy, Microsoft
8) Kaja Ciglic, Senior Director, Digital Diplomacy, Microsoft
9) Antonio Coco, Lecturer in Public International Law, University of Essex and Visiting Fellow at ELAC, University of Oxford
10) Gary Corn, Professor of Law and Director of Technology, Law & Security Program, American University Washington College of Law
11) Rebecca Crootof, Assistant Professor of Law, University of Richmond School of Law
12) François Delerue, Research Fellow in Cyberdefense and International Law, Institute of Strategic Research of the Military Academy, France
13) Miguel de Serpa Soares, Under-Secretary-General for Legal Affairs, The United Nations Legal Counsel
14) Talita Dias, Research Fellow, Jesus College & ELAC, University of Oxford
15) Kristen Eichensehr, Martha Lubin Karsh and Bruce A. Karsh Bicentennial Professor of Law, University of Virginia
16) David Fidler, Adjunct Senior Fellow for Cybersecurity & Global Health, Council on Foreign Relations
17) Mohamed Helal, Associate Professor of Law, Moritz College of Law and Member, African Union Commission on International Law (2020-2025)
18) Heikki Hietala, Senior Specialist, Permanent Representation of Finland to the European Union
19) Duncan Hollis, Laura H. Carnell Professor of Law, Temple University School of Law

20) Zhixiong Huang, Professor of International Law and Vice Dean for International relations, Executive Director, Wuhan University Institute for Cyber Governance, Wuhan University
21) Graham Ingram, Chief Information Security Officer, University of Oxford
22) Kate Jones, University of Oxford
23) Andraz Andy Kastelic, Lead cyber stability researcher, Security and Technology Programme, UNIDIR
24) David Kaye, Clinical Professor of Law, University of California, Irvine
25) Harold Hongju Koh, Senior Adviser and former Legal Adviser (2009-13), Office of the Legal Adviser, US Department of State
26) Jeffrey Kovar, Assistant Legal Adviser for Political-Military Affairs, US Department of State
27) Chris Krebs, Partner, Krebs Stamos Group LLC
28) Leonhard Kreuzer, Research Fellow, Max Planck Institute for Comparative Public Law and International Law
29) Joanna Kulesza, Professor of Law, University of Lodz
30) Masahiro Kurosaki, Associate Professor of International Law and Director of the Study of Law, Security and Military Operations, National Defense Academy of Japan
31) Henning Lahmann, Senior Researcher, Digital Society Institute, ESMT Berlin
32) Noam Lubell, Professor of Law, University of Essex and Director, Essex Armed Conflict and Crisis Hub
33) Asaf Lubin, Associate Professor of Law, Indiana University Maurer School of Law
34) Kubo Mačak,Legal Adviser, ICRC and Associate Professor, University of Exeter
35) Nemanja Malisevic, Director, Digital Diplomacy International Lead, Defending Democracy Program, Microsoft
36) Ciaran Martin, Professor of Practice in the Management of Public Organisations, Blavatnik School of Government
37) Tomohiro Mikanagi, Deputy Director-General of the International Legal Affairs Bureau, Ministry of Foreign Affairs of Japan
38) Marko Milanovic, Professor of Public International Law, University of Nottingham
39) Tomáš Minárik, Head of International Organisations and Law Unit, National Cyber and Information Security Agency of the Czech Republic
40) Harriet Moynihan, Associate Fellow, Royal Institute of International Affairs (Chatham House)

41) Jan Neutze, Senior Director, Digital Diplomacy, Microsoft
42) Elina Noor, Director, Political-Security Affairs and Deputy Director, Asia Society Policy Institute
43) Kazuho Norikura, Ministry of Foreign Affairs, Japan
44) Jim O'Brien, Vice Chair, Albright Stonebridge Group
45) Jens Ohlin, Allan R. Tessler Dean & Professor of Law, Cornell Law School
46) Andrés Ordoñez-Buitrago, Second Secretary, Ministry of Foreign Affairs, Colombia
47) Harry Ormsby, Assistant Legal Adviser, National Security Team, Legal Directorate, Foreign, Commonwealth and Development Office
48) Christian Perrone, Coordinator of the Rights and Technology Group, Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS)
49) Patryk Pawlak, Executive Officer, European Union Institute for Security Studies
50) Michael Schmitt, Professor of International Law, University of Reading; Francis Lieber Distinguished Scholar at the Lieber Institute of the United States Military Academy (West Point)
51) Lucía Solano, Legal Adviser, Permanent Mission of Colombia to the United Nations in New York
52) Hansjoerg Strohmeyer, Chief of Policy Development and Studies Branch, United Nations Office for the Coordination of Humanitarian Affairs
53) Nikhil Sud, Regulatory Affairs Specialist, Albright Stonebridge Group
54) Arun Mohan Sukumar, Head, Cyber Initiative, Observer Research Foundation and PhD candidate, Fletcher School of Law & Diplomacy, Tufts University
55) John Swords, Legal Adviser and Director of the Office of Legal Affairs at NATO Headquarters
56) Emily Taylor, Associate Fellow, International Security Programme, Chatham House
57) Joel Trachtman, Henry J. Braker Professor of Law, The Fletcher School of Tufts University
58) Tsvetelina van Benthem, Research Officer, ELAC
59) Liis Vihul, Chief Executive Officer, Cyber Law International
60) George W, GCHQ
61) Marguerite Walter, Attorney-Adviser, Human Rights and Refugees, Office of the Legal Adviser, US Department of State

62) Alexander Wentker, DPhil candidate in International Law, University of Oxford
63) Stephen Wheatley, Professor of International Law, University of Lancaster
64) Briony Daley Whitworth, Assistant Director, Cyber Affairs Branch, Department of Foreign Affairs and Trade, Australia
65) Robert Young, Legal Counsel, Global Affairs Canada

Appendix: Four case studies on ransomware

Background: Zaphod is a well-known hacker group, which has been involved in dozens of large-scale ransomware operations, impacting governments, critical infrastructure providers, international organisations and corporations around the world. There are some indications that Zaphod maintains strong connections with the State of Damogran. While Damogran has denied such claims, the methods used by the hackers closely track methods that have been attributed to the security agency of Damogran. Despite evidence that the group operates from the territory of Damogran, no investigations have yet been initiated by the State of Damogran.

Hypo 1: In early July 2021, Zaphod identified a vulnerability in the network management software of Vogon, a software company incorporated in The Republic of Betelgeuse. Zaphod introduced a backdoor through which it pushed a ransomware payload[1] to the clients of Vogon, which include a number of governmental agencies, educational institutions and healthcare providers in Betelgeuse. To gain a universal decryptor and recover their data, the victims were asked to pay 50 million GBP. There have been allegations that the money is used to finance terrorist and secessionist activities in the traditionally violent and underdeveloped Global North. Several schools, universities and hospitals did not pay immediately, which led to an interruption of teaching and medical treatments. Three governmental agencies, however, paid the ransom within 24 hrs, and were able to access their data. It was later established that the vulnerability in Vogon's systems had been known to both the company and its government clients for over three months, and yet no patch to that vulnerability had been issued by the time of the attack.

Hypo 2: In March 2021, the group attacked a research institute conducting clinical trials on a new vaccine for Covid-19. Following this ransomware attack, the research institute was unable to continue the trials for three weeks.

Hypo 3: Later, in May 2021, a water filtration facility became the victim of a ransomware attack. Its systems were accessed through one single compromised password,[2] which had been leaked on the Dark Web. Zaphod sent a ransomware note, and the management of the water filtration facility decided to shut down its operations immediately. In the process of rapidly shutting down the facility, a leak of sodium hydroxide was observed.[3] While there had been no reports of poisoning in the neighbouring community, sodium hydroxide can cause burns and bleeding. In the months prior to this attack, many other critical infrastructure providers had been hacked through compromised passwords.

Hypo 4: On July 10, 2021, the Betelgeuse Ministry of Foreign Affairs and its national healthcare provider suffered a major ransomware incident, following a period of tensions with Damogran over the arrest of a Damograni national. The Ministry's activities were disrupted, and delays caused by the operations led to the death of 17 patients in Betelgeuse. In the ransomware note sent to the Ministry, the officials were asked to release the Damograni national and extradite him to his State of nationality. Failure to comply, according to the note, would lead to 'more delays in the healthcare system and more deaths'. The Betelgeuse cybersecurity agency submitted a report to the President, stating that the evidence strongly suggests the involvement of a State actor, and that the method used mirrors techniques employed by Damogran. As a response, the President of Betelgeuse formally attributed the attack to Damogran and gave the State 24 hours to provide the decryption key. She further asserted that, unless they are given the decryption key, Betelgeuse will launch a military strike against Damogran and impose economic sanctions in breach of their trade agreement.

Primer for the Oxford Process on the:

Regulation of Ransomware under International Law:
1) what is ransomware?
2) a malware lifecycle;
3) current state of ransomware;
4) sample events.

20 July 2021

*Graham Ingram**

* Chief Information Security Officer, University of Oxford

1. Ransomware.

Ransomware is a type of malware that prevents you from accessing your computer (or the data stored on it). Typically, files are rendered unusable by an encryption algorithm, but data may also be stolen and released online.[1] Usually, the cryptographic malware affects entire networks, including servers and user devices. A message is displayed on your computer which invites you to pay a ransom (often in crypto currency) to have your files unlocked. An attacker will have spent some time on the network, attempting lateral movement, to:

a. Acquire Key Data. An increasing Tactic, Technique & Procedure (TTP) for cyber-criminals is to identify and remove key data. This increases the likelihood that victims will pay to prevent damage caused by release of that data, including costly sanctions from privacy regulators.

b. Map the Network. Attackers will seek to understand the networks so that they can infect as many devices as possible. The attacker must balance dwell time on the networks with the risk of detection. The more widespread the infection, the more likely the victim will be inclined to pay.

c. Identify the Backups. Restoration from back-ups is the last line of defence for victims. An attacker will seek to poison these back-ups and leave an organisation no option but to pay.

d. Race to publicise. Ransomware purveyors are increasingly using the publication of the stolen data as an event to publicise their achievements. Victim organisations are normally inclined to keep quiet about cyber intrusions; now there is a race to own the narrative.

1 "Ransomware: What board members should know and what they should be asking their technical experts." United Kingdom National Cyber Security Centre: Hannah H. 2 June 2021.

2. Kill Chain.

The delivery of ransomware is not an isolated act of malicious activity. It is the culmination of an extensive cyber effort requiring unauthorised access to computer networks before achieving the goal (to monetize the attack). Ransomware is just one of the options in the toolkit open to the attacker during the last three stages of the attack. The attacker may trade access, deploy other tools, or seek the expertise of others (such as 'Ransomware as a Service' providers) from the Darkweb. There is no fixed timeframe for this chain of events in Figure 1[2]; the more sophisticated the attackers, the longer they can spend hiding on the network deleting logs as they go. There may be gaps of hours to months between these steps.[3]

Figure 1: Lockheed Martin Cyber Kill Chain reproduced from "Breaking the Attack Kill Chain" white paper from Palo Alto Networks

3. The global rise of ransomware.[4]

a. Ransomware attacks have increased 485% from 2019 to 2020.

b. 34% of organisations have paid ransoms; it is likely that this is fuelling the business model.

c. If cyber insurance is in place, the decision to pay potentially belongs to the underwriter.

2 "Breaking the Attack Kill Chain." Pal Alto Networks white paper September 03, 2015.
3 "Most ransomware attacks take place during the night or over the weekend." Catalin Cimpau on ZDNet; March 16, 2020.
4 "Tips To Strengthen Your Ransomware Defences in Education." Paul Furtado; Owen Pengelly: Gartner webinar 9 Jul 2021.

d. The incidence of Doxing (publication of stolen data) has risen from 16% of attacks to 77% attacks in the last year.

e. Disruption caused by such an attack can be five to ten times the cost of the payment.

f. 58% of attacks now require further payments; some or all of the data may not be unlocked.

g. Organisations that pay, and receive the key, still lose 4% of their data and are off-line on average for 23 days.

h. Ransomware is deployed somewhere in the world every 11 seconds.

4. High profile attacks.

a. 2017: WannaCry ransomware infected around 230,000 computers globally across 150 countries with an estimated global financial impact of $4Bn. In the UK, it had a serious impact on the National Health Service with an estimated cost of £92 million and caused the cancellation of 19,000 appointments.[5] It was attributed to a North Korean cyber group;[6] if any ransom payments were made, they may have breached international sanctions.[7]

b. 2017: NotPetya appeared to be a ransom demanding malware attack. But it was not configured to track payments and provide the decryption key in return. This attack, attributed to a Russian state actor[8] used the update servers to a business accounting service 'MEDoc' to paralyse Ukrainian agencies. It impacted many other users of this software package including the shipping giant AP Møller-Maersk[9] who reported losses of $300m due to the incident. Several companies, including Mondelez (the owners of Oreo, Cadbury and Kenco), were frustrated in claiming against

5 "What is WannaCry ransomware?" Kaspersky Resource Centre; last accessed 10 July 2021.
6 "U.S. charges North Korean hacker in Sony, WannaCry cyberattacks." Bing & Lynch of Reuters; last accessed 10 July 2021.
7 "Treasury Department Warns of Sanctions Risks if Facilitating or Paying a Ransomware Payment." HIPAA Journal Oct 2020.
8 "Russian State 'almost certainly' responsible for destructive 2017 cyber attack" NCSC news dated 14 February 2018.
9 "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." Andy Greenberg; Wired.com 22 August 2018.

their cyber insurance as a 'war exclusion' clause was invoked.[10]

c. 2020: German prosecutors open a homicide case after a ransomware attack on a Düsseldorf hospital. A patient suffering from a life threatening illness was re-directed to another hospital 30km away after the Düsseldorf university clinic was unable to accept the patient.[11] Although this was widely reported as the first death directly attributed to a cyber-attack, police investigations concluded that, as the patient was in such poor health, the time delay in treatment due to the ransomware attack did not alter the outcome.[12]

d. 2021: Recently Irish Healthcare services were severely impacted by a significant ransomware attack causing a detrimental impact to most services from maternity cover to cancer care.[13] The 'Conti' ransomware group subsequently offered the decryption key to allow the restoration of healthcare operations, but they continued with a $20M demand to delete stolen sensitive data.[14]

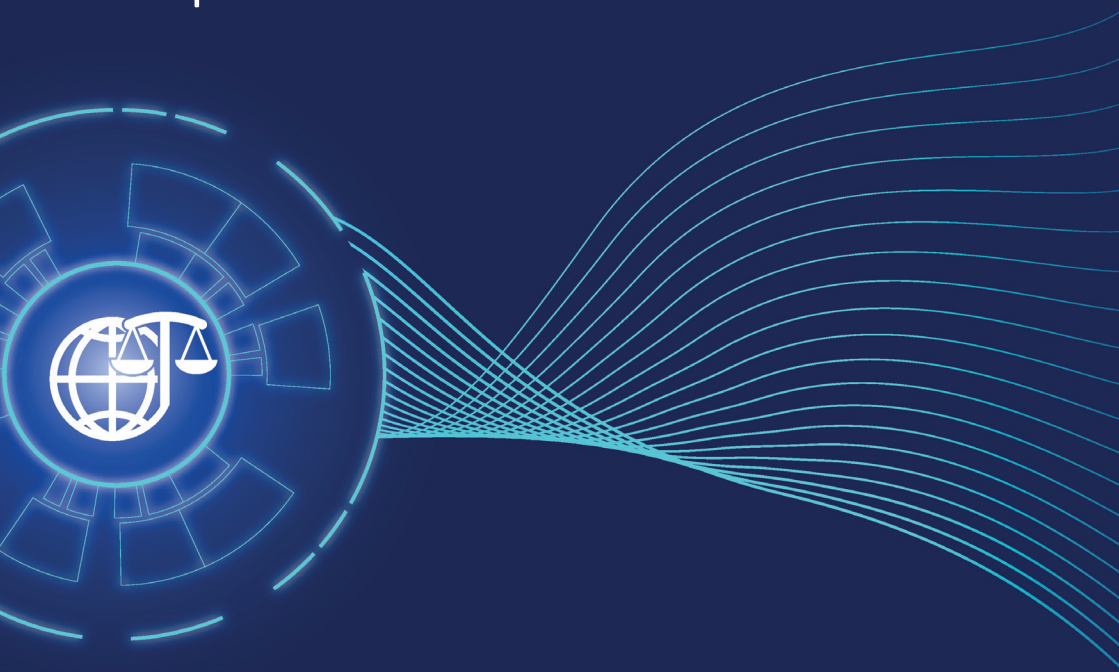
e. 2021: Kaseya Virtual System Administrator (VSA) is a widely used IT management, automation and security package. Earlier this month it was compromised by an organised cyber-criminal group based in Russia called REvil.[15] This supply chain attack has caused more than 1,000 Kaseya customers in 17 countries to endure ransomware infections.[16] REvil have offered a central decrypt key for $70M.

5. An excellent visualisation of the growth of the problem is here: Ransomware Attacks — Information is Beautiful; allow the web page a few seconds to load, click on a bubble to retrieve more detail.

10 "Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong." Satariano and Perlroth; New York Times, 15 April 2019.
11 "Prosecutors open homicide case after hacker attack on German hospital" Reuters; 18 September 2020.
12 "Ransomware did not kill a German hospital patient." Patrick Howell O'Neill; MIT Technology Review. November 12, 2020.
13 "Number of days before systems are back working – HSE" RTE dated 17 May 2021.
14 "Irish Health Service Hackers Offer Decryption Key – but $20M Ransom Demand Remains." Gallagher and Flanagan; Insurance Journal: May 21, 2021.
15 "CISA-FBI Guidance for MSPs and their Customers Affected by the Kaseya VSA Supply-Chain Ransomware Attack." U.S. Cybersecurity & Infrastructure Security Agency dated July 04, 2021.
16 "A massive ransomware attack hit hundreds of businesses. Here's what we know" Clare Duffy, CNN Business; July 07, 2021.

7 The Oxford Process on International Law Protections in Cyberspace: Countermeasures in Cyberspace

Workshop
Report



The Oxford Process on International Law Protections in Cyberspace:

Countermeasures in Cyberspace

12 May 2022

Executive Summary & Key Takeaways

On Thursday May 12th, 2022, the Oxford Institute for Ethics, Law and Armed Conflict (ELAC) held a workshop, sponsored by Microsoft and the Embassy of Japan in the United Kingdom, on the international legal regulation of countermeasures in cyberspace. This workshop was part of the Oxford Process on International Law Protections in Cyberspace, an initiative seeking to identify points of consensus on international legal rules and principles in their application to specific sectors, objects and activities. This workshop was the seventh one in the Oxford Process series.

The doctrine of countermeasures as a circumstance precluding wrongfulness is well-established in international law. And while international law permits a state to resort to countermeasures when it is directly injured as a result of the breach by another state of obligations owed by the latter state to the former, important controversies remain around the procedural requirements for the taking of countermeasures, as well as the possibility of non-injured States to resort to countermeasures. The resort by States to countermeasures, whether individually or collectively, raises complex questions in the cyber context. The following points emerged from the discussion:

1. The law of State responsibility applies to cyberspace.

2. While States do not dispute the existence of procedural requirements associated with the taking of countermeasures under general international law, they sometimes merge the requirements of sommation and notification. This has become particularly obvious in cyberspace, where States are currently advancing or developing their positions regarding whether, and if so how, procedural requirements can be dispensed with, whether as a cyberspace lex specialis or as a lex specialis application of the urgent countermeasures exception.

3. The legality of the resort to collective countermeasures is still hotly debated among both States and academics. Even if State practice comes to coalesce around the legality of such countermeasures, more work is needed to determine the types of violations that would enable the taking of such countermeasures and the application of the proportionality requirement to collective action, among others.

Background

The Oxford Process on International Law Protections in Cyberspace has since May 2020 brought international lawyers, cyber experts, state representatives, representatives of international organisations, civil society and industry together to discuss how international law applies to cyber operations. As part of this endeavour, and in the light of ongoing Russian aggression in Ukraine, the workshop addressed the permissibility under international law of countermeasures taken by states in the context of cyber operations.

International law permits a state to resort to countermeasures when it is directly injured as a result of the breach by another state of obligations owed by the latter state to the former. The wrongfulness of these measures – which would, under ordinary circumstances, themselves constitute a breach of international law – is precluded by the fact of the prior breach. Amongst various other procedural requirements specified by the International Law Commission (ILC) in its 2001 Articles on the Responsibility of States for Internationally Wrongful Acts, countermeasures must be taken with a view to inducing the state in breach to comply with its obligations. Beyond this, there is little clarity as to the conditions under which countermeasures are permitted under international law. The resort by states to countermeasures, whether individually or collectively, raises additional questions in the cyber context, particularly how the relevant procedural requirements might be satisfied therein.

Clarification is also required as to whether, and under which conditions, a state may take countermeasures in response to breaches of

international law, when the state taking the measures is not directly injured by the breach. The 2001 ILC Articles left unanswered whether third states may take countermeasures in response to breaches of obligations erga omnes (so called 'third party countermeasures'). Similarly, there has been much discussion of whether third states that are not directly injured may take 'collective countermeasures' at the request of the state that is directly injured. While some states, like Estonia and New Zealand, refer to asymmetries in states' cyber capabilities to make the case for collective countermeasures, others, like France, consider collective cyber countermeasures to be unlawful. Clarity is urgently needed given the increasing resort by states to cyber operations in response to breaches of international law. This was evidenced by the range of cyber operations being undertaken against Russia in response to cyber operations against the Ukrainian government, military, banks and other private sector networks since January 2022, as well as kinetic military operations. Along with the possibility of responding by cyber means to unlawful non-cyber measures, states may wish to respond to unlawful cyber operations with collective non-cyber measures.

The workshop addressed these various issues by undertaking two lines of inquiry:

First, what are the preconditions and procedural requirements that must be satisfied for the resort by states to countermeasures? How might these requirements be satisfied in the cyber context and what cyber-specific difficulties arise?

Secondly, are states permitted to undertake collective or third-party countermeasures? Is it necessary that these countermeasures, if permitted, be taken in response to violations of erga omnes obligations (as in the case of Ukraine), or may they also be taken at the request of an injured state even absent breaches of obligations erga omnes?

Each line of inquiry was pursued in a dedicated session of the workshop.

Summary of Sessions

Welcome and Introduction

Professors Dapo Akande (ELAC) and Duncan Hollis (Temple University) gave the introductory remarks, presenting the Oxford Process to the workshop participants. Through expert discussions, the Oxford Process seeks to specify the application of international law to particular means and objects of protection, thus identifying areas of consensus on the scope of applicable rights and obligations. While the Oxford Process is firmly grounded in the discipline of international law and seeks to outline protections under existing law, it is also oriented towards the shaping of state behaviour.

The goal of this workshop was to examine how States might use countermeasures to respond to international wrongs, with a particular focus on state conduct in cyberspace. An inquiry of particular relevance was the fit between general international law and the way States are shaping their legal claims in the area of cyber countermeasures, that is, both countermeasures taken in response to cyber operations and cyber operations taken in response to any prior internationally wrongful act. The Convenors urged the participants to examine points of consensus as well as areas where State practice seems to diverge.

Session I

Cyber Countermeasures: Procedural Requirements

Moderated by Professor Dapo Akande, ELAC

Presentation: Przemysław Roguski, Lecturer in Law, Jagiellonian University, Kraków

This presentation focused on the procedural requirements associated with the taking of countermeasures against harmful cyber operations. Dr Roguski explored this topic against the background of discussions on the procedural requirements of countermeasures generally, as well as of emerging state practice on countermeasures that is specific to cyberspace. As a preliminary point, Dr Roguski noted that there is majority agreement among States to the effect that the law of State responsibility, including

countermeasures, applies to cyber operations. Because of the peculiarities of cyberspace, however, certain States, such as Brazil, advocate for a cautious approach to the applicability of countermeasures.

Turning to the procedural requirements, the ILC's Articles on State Responsibility, in Art. 52, list two main procedural conditions relating to resort to countermeasures: sommation, on the one hand, and notification and offer to negotiate, on the other.

The requirement of sommation obliges the injured State to first call upon the State committing the wrongful act to discontinue its wrongful conduct or to make reparation for it before instituting countermeasures. International bodies have confirmed the existence of this requirement as part of customary international law. This procedural condition seeks to both provide an opportunity to the responsible State to review its conduct, and to safeguard it from abusive or premature countermeasures.

The requirement of notification of the intent to take countermeasures and the offer to negotiate stands on less established legal ground. This procedural condition was the subject of intense controversy at the ILC, its final wording a compromise seeking to accommodate the fact that the actual conduct of negotiations would require cooperation from the responsible State. The Articles on State Responsibility provide an exception to this procedural obligation, however. They envision the taking of urgent countermeasures by an injured State where such countermeasures are necessary to preserve its rights. Thus, in case of urgent countermeasures, the injured State can dispense with the second procedural requirement, that is, the requirement of notification and the offer to negotiate. Importantly, this dispensation only concerns the second procedural requirement, but not the first, that of summation.

In his assessment of State practice, Dr Roguski noted that many States do not clearly distinguish between the requirement of sommation and the requirement of notification and offer to negotiate. This may be due

to the lack of particular sequencing between the requirements, and the possible discharging of both through the same act. Nevertheless, because of their different purposes and orientation, as well as the dispensation from the notification requirement only for urgent countermeasures, the two need to be kept conceptually separate.

According to Dr Roguski, when it comes to responding to cyber operations, some trends in the practice of States may evince a departure from the procedural requirements as outlined by the ILC. Israel and the United Kingdom, for instance, put into question the duty to notify the responsible State in advance of a cyber countermeasure, while the United States views the necessity of a 'prior demand' on the responsible State as contingent on the particular circumstances of the situation at hand. The position of Israel and the United Kingdom departs from existing international law, as currently interpreted, and may thus seek to establish a cyber-specific exception to the sommation requirement. A more modest position advanced by some States is that the sommation requirement is also subject to the urgent countermeasures exception. Dr Roguski concluded his remarks by highlighting that, to achieve greater clarity in this area, more States should come forward with their positions on the procedural conditions for the taking of countermeasures.

Discussant: Professor Kimberley Trapp, Professor of Public International Law, University College London

In her remarks, Professor Trapp focused on three main points: questions of vocabulary; a note on context and purpose; and State concerns over procedural requirements. By way of conclusion, Professor Trapp noted a seeming shift towards a self-defence oriented lens to the application of countermeasures.

On vocabulary, it was noted that it was not always clear that States were using 'countermeasures' in the public international law sense – which is to say as a circumstance precluding the wrongfulness of conduct,

otherwise in breach of international law, which responds to a prior internationally wrongful act. States sometimes seemed to be referring to a directly responsive, defensive and protective measure – irrespective of whether the measure breached international law.
Turning to purpose and context, Professor Trapp reminded that the ILC's Articles frame countermeasures in instrumental terms – to restore the primary legal relationship as between the injured and wrongdoing States which has been ruptured by the wrongdoing State's internationally wrongful act, and that the logic of the procedural requirements for the adoption of countermeasures (sommation, notification and offer to negotiate) reflects the instrumental and systemic elements of countermeasures. In her view, the ILC's final position on countermeasures was a balancing act – with a view to creating / preserving the space for an amicable solution, decreasing the chances of escalation / spiralling countermeasures, and avoiding the risk of abuse by the measure adopting (injured) State while avoiding giving the wrongdoing State a veto over the adoption of countermeasures against it.

On particular State concerns, Professor Trapp noted that States expressed various views about the applicability and or suitability of the countermeasure procedural requirements to the cyber context.

States expressed concern regarding the impact of procedural requirements, in particular prior notice, on the effectiveness of countermeasures. Professor Trapp noted that from a purely international law standpoint, we should measure the effectiveness of countermeasures against their instrumental objectives, but that States seemed to also, and principally be thinking of effectiveness in terms of halting, repelling or otherwise protecting against a cyber operation. Professor Trapp further noted that issues of covertness were raised in State comments on the procedural requirements – either the covert nature of the prior internationally wrongful act or the covert nature of the cyber response (with possibly sommation but certainly notification as required by Art. 52 revealing the countermeasure adopting State's

own cyber capabilities which, for security reasons, are better kept secret). The comments seem to suggest that some form of national security type exception needs to contemplated for either sommation or prior notification (or both) depending on the circumstances. Professor Trapp noted that these concerns do not seem to be an issue with prior notice, but with notice requirements, full stop. And if that is the case – the purpose and structure of countermeasures, which calls for a fair measure of transparency, is undermined.

Professor Trapp concluded that State concern over effectiveness and national security / covertness suggested that the paradigm being invoked is not that of countermeasures at all, but something more like a right of cyber-defence – precluding the wrongfulness of a responsive measure, but with a defensive aim rather than an instrumental aim of re-establishing the primary legal relationship.

Discussant: Ashley Deeks, Associate White House Counsel and Deputy Legal Advisor, US National Security Council and University of Virginia

Professor Deeks engaged in a legal inquiry into the relationship between the procedural requirement of sommation and the notion of 'preservation of rights' under the urgent countermeasures doctrine. According to her, a straightforward textual analysis indicates that the requirement of sommation stands. That said, the practice of States suggests that sommation is subsumed under the exception applicable to urgent countermeasures.

Professor Deeks further inquired whether the requirement of sommation could be satisfied through a general, rather than a specific statement. An example of an *ex ante* could be a State providing an *ex ante* blanket statement that it would treat interferences with vote counts as a customary international law violation that would warrant countermeasures.

Finally, Professor Deeks addressed a temporal question: when can we say that the wrongful act has ceased? This question gains a particular importance in pinprick scenarios with clusters of cyber operations.

For further reflections by Professor Deeks on the regulation of cyber countermeasures under international law, the participants were directed to Ashley Deeks, 'Defend Forward and Cyber Countermeasures' (2020).

Open discussion

During the open discussion, the participants raised six main thematic issues.

First, as a note on terminology, it was highlighted that the term 'countermeasure' is being used to both denote a legal concept and a technical one (that is, technical efforts to stop a cyber operation). These two meanings must be clearly separated to avoid conflation.

Second, it was queried whether the regulation of countermeasures, as outlined in the Articles on State Responsibility, is sufficient, or even adequate, to address the contemporary reality of cyber operations. According to some, there is a need to develop a lex specialis applicable to cyberspace.

Third, the participants debated the purpose of countermeasures, as understood by States and international bodies. While the Articles on State Responsibility speak of a goal of inducing compliance with international obligations, some governments seem to adopt a punitive lens to the taking of countermeasures. A particular point of contention was whether 'to induce compliance' means forcing the will of a State or placing it in a position where it cannot act any further.

Fourth, and turning to the specific procedural requirements of sommation and notification, most participants affirmed their separate

existence and significance. For some, a law on countermeasures without robust procedural requirements would go against the principle of pacific settlement of disputes. While there was wide agreement that sommation cannot be dispensed with through urgent countermeasures, one participant advanced the view that the requirement can be dispensed with if it had been discharged previously in general terms. This, then, raised additional questions of whether sommation can be done in a general way.

Fifth, the desirability of anticipatory countermeasures was debated, and ultimately rejected. Most participants agreed that it would be better to create new primary international obligations prohibiting risky behaviour rather than to extend the scope of secondary rules of international law on circumstances precluding wrongfulness. It was also noted that the current developments in State positions on countermeasures may influence the specification of primary rules of international law.

Sixth, and turning to risks, participants highlighted concerns over the taking of countermeasures in circumstances where the responding State is mistaken about the identity of the perpetrator, or about factors relevant to the alleged prior internationally wrongful act. These risks are heightened in cyberspace, in particular because of the difficulties with attribution. Because of the escalatory potential of countermeasures, and specifically mistaken countermeasures, it was concluded that the procedural requirements have an important function to play in constraining State behaviour.

Session II

Collective Countermeasures in Cyberspace

Moderated by Professor Duncan Hollis, Temple Law School
Presentation: Lori Fisler Damrosch, Hamilton Fish Professor of International Law and Diplomacy, Columbia University

The presentation examined the legality of collective countermeasures under existing international law, as well as the desirability of this enforcement tool in view of achieving broader normative goals. To begin with, Professor Damrosch clarified that while the term 'collective countermeasures' is often used in the literature, it has no authoritative definition under international law. The compromise language contained in the Articles on State Responsibility left the question of the legality of collective countermeasures unanswered, thus leaving space for developments through the practice of States.

In the absence of an agreed meaning of 'collective' countermeasures, one option might be to make an analogy with the regime of collective self-defence, which allows third-party uses of force in response to an armed attack. Under this analogy, criteria relevant for collective self-defence might arguably apply to the taking of collective countermeasures: for example, (1) a State might have to declare itself to have been injured by an internationally wrongful act; (2) that State might have to request the assistance of other States; (3) the assisting States would have to act within the bounds of the request; and (4) the assistance would have to comply with other relevant requirements, such as proportionality. Another possible analogy for collective countermeasures would be the collective security paradigm. According to Professor Damrosch, both analogies are of limited use, as they concern conditions developed to restrain forcible responses to forcible wrongs.

The overarching argument advanced by Professor Damrosch was that collective cyber countermeasures in support of injured States are lawful. First, this position was seen as supported by normative goals. This permissive view would not only enable smaller States to seek assistance

against more powerful offenders, but it would further demonstrate international commitment to the international legal system and thus deter wrongful conduct. Second, Professor Damrosch found support for this argument in the practice of States, in particular in the area of diplomatic and consular law, but also potentially in non-proliferation and anti-terrorism regimes. In the area of diplomatic and consular law, the economic measures taken by United States' allies in response to the Tehran hostage crisis were highlighted. And in the area of non-proliferation and anti-terrorism regimes, the presentation covered examples of domestically imposed sanctions. For all these obligations, it was considered that violations can easily be committed in cyberspace.

Professor Damrosch addressed a number of specific controversies regarding the legality of countermeasures taken by a State that is not directly injured by the breach. First, she examined the question to whom the obligations are owed, emphasising the important developments in the area of *erga omnes* and *erga omnes* partes obligations. Second, she queried the hierarchical superiority of certain obligations, that is, of obligations with a *jus cogens* status. The recent work of the International Law Commission on the study of peremptory norms was mentioned. And finally, Professor Damrosch inquired into the test of 'serious breach', highlighting the special consequences entailed, under the law of State responsibility, for serious breaches of peremptory norms, such as duties of cooperation.

In her concluding remarks, Professor Damrosch considered that the view that only injured States can lawfully respond through countermeasures would leave a large enforcement gap. If cautiously specified and applied, collective countermeasures can strengthen the international legal system.

Discussant: Harriet Moynihan, Associate Fellow, Chatham House

Beyond the ILC's Articles on State Responsibility, which do not conclusively answer the question of the permissibility of collective

countermeasures, Ms. Moynihan suggested that while state practice and *opinio juris* should inform the legal assessment, underlying legal policy considerations should also be considered. First, she noted the absence of sufficient state practice and *opinio juris* in the cyber context so far, with only New Zealand, France and Estonia expressing a view on the topic. Secondly, while being mindful of the exceptional nature of countermeasures, and of the conditions governing use of countermeasures in the ILC's Articles, she also noted the need for States to be able to respond appropriately in the face of cyber operations that violate international law, and the lack of capacity of some victim States to do so.

Ms Moynihan noted the lack of clear boundaries of the category of *erga omnes* obligations. She also emphasised the need to distinguish between collective and third-party countermeasures.

Discussant:John Swords, Legal Adviser and Director of the Office of Legal Affairs, NATO

Mr. Swords, speaking in his personal capacity, noted the tendency of some practitioners to view collective countermeasures on a spectrum of potential response options somewhere between collective retorsions and collective self-defence. He noted the desirability of distinguishing the use of countermeasures by states other than injured states in response to violations of obligations erga omnes, from the variety of measures taken in response to requests for assistance by injured states absent erga omnes violations. He noted that it is not always clear from the outside whether or not states are acting on the basis of such countermeasures, or whether they are simply invoking exceptions to certain obligations within the relevant treaties or invoking principles set out in the VCLT. He noted some of the legal policy reasons sometimes cited in support of forms of collective countermeasures, namely when a victim state lacks the capability or political will to react unilaterally. He noted that a requirement for an erga omnes violation is attractive to some, both as a matter of principle and as a sensible guardrail. He

wondered how much sense that requirement made in practice, if third states could continue to give material aid and assistance to victim states to enable them to exercise their own undoubted rights.

Open discussion

During the discussion, the participants focused on four strands of the broader collective countermeasures debates.

First, a point of contention was the nature of international law violations that enable the taking of collective countermeasures. Can collective countermeasures be taken in response to any violation of international law? To only certain obligations and regimes? To only obligations established in the interest of the international community as a whole? Within this discussion, the participants noted the uncertainty around the criteria for determining whether an obligation falls within the *erga omnes* and *erga omnes* partes categories.

A second question concerned the taking of collective countermeasures not only as a permissible avenue for action, but also as a required course of action. This might be the case where the obligation in question is an erga omnes obligation pertaining to a *jus cogens* norm.

Further, it was debated how one is to assess the requirement of proportionality in the context of collective countermeasures. Should the overall impact of such countermeasures be proportionate to the injury suffered by the injured State? If so, how can collective responses be synchronised? Some participants were of the view that the proportionality requirement may entail a duty of cooperation in the sphere of collective countermeasures.

A final line of inquiry concerned the relationship between the taking of collective countermeasures, the attribution ground of organs placed at the disposal of another State, and the permissibility of aid and assistance to an injured state, as opposed to collective countermeasures, as a

permitted course of action.

Concluding remarks

In his concluding remarks, Professor Harold Hongju Koh pointed to the importance of the timing of the workshop, taking place during the war in Ukraine, at a time when States are considering all international legal tools in their arsenal to induce compliance and deter future breaches of the law.

Despite the complexity of the topic of countermeasures, Professor Koh noted that the discussion clearly pointed to areas of consensus, as well as to areas in flux, where the practice of States is currently shaping the content of international legal rules.

List of Participants

1. Dapo Akande, ELAC, Blavatnik School of Government, University of Oxford
2. Danae Azaria, Faculty of Laws, University College London
3. Russell Buchan, School of Law, University of Sheffield
4. Scott Charney, Microsoft
5. Shehzad Charania, GCHQ
6. Mary Chong, Attorney-General's Chambers, Singapore
7. Kaja Ciglic, Microsoft
8. Antonio Coco, School of Law, University of Essex
9. Gary Corn, American University Washington College of Law
10. Rebecca Crootof, University of Richmond School of Law
11. Lori Fisler Damrosch, Columbia University
12. Martin Dawidowicz, Uppsala University
13. Ashley Deeks, US National Security Council and University of Virginia
14. François Delerue, Institute of Security and Global Affairs, Leiden University
15. Talita Dias, Jesus College and ELAC, University of Oxford
16. Kristen Eichensehr, University of Virginia School of Law
17. Yuka Fukunaga, Waseda University
18. Samuli Haataja, Griffith University
19. Yusuke Hatakeyama, Embassy of Japan in the United Kingdom
20. Oona Hathaway, Yale Law School
21. Mohamed Helal, Ohio State University Moritz College of Law
22. Duncan B. Hollis, Temple Law School
23. Zhixiong Huang, Wuhan University
24. Miles Jackson, Law Faculty, University of Oxford
25. Taťána Jančárková, NATO Cooperative Cyber Defence Centre of Excellence
26. Triinu Kallas, Ministry for Foreign Affairs, Estonia
27. Harold Hongju Koh, Yale Law School
28. Jeff Kosseff, Cyber Science Department, United States Naval Academy
29. Maroi Kouka, Université Paris 8
30. Masahiro Kurosaki, National Defense Academy, Ministry of Defense, Japan
31. Vladyslav Lanovoy, Université Laval
32. Asaf Lubin, Indiana University Maurer School of Law

33. Georgina Lupson, Department of Foreign Affairs and Trade, Australia
34. Nemanja Malisevic, Microsoft
35. Ekaterina Martynova, National Research University Higher School of Economics
36. Neil McDonald, Attorney General's Office, United Kingdom
37. Ulf Melgaard, Ministry of Foreign Affairs, Denmark
38. Tomohiro Mikanagi, International Legal Affairs Bureau, Ministry of Foreign Affairs, Japan
39. Harriet Moynihan, Chatham House
40. Tomáš Minárik, National Cyber and Information Security Agency, Czech Republic
41. Jan Neutze, Microsoft
42. Jens David Ohlin, Cornell Law School
43. Harry Ormsby, Foreign, Commonwealth and Development Office
44. Martins Paparinskis, Faculty of Laws, University College London
45. Nish Perera, Department of Foreign Affairs and Trade, Australia
46. Andrea Raab, ICRC
47. Przemysław Roguski, Jagiellonian University, Kraków
48. Nicola Smith, Foreign, Commonwealth and Development Office
49. Lucía Solano, Permanent Mission of Colombia to the United Nations in New York
50. Marcus Song, Attorney-General's Chambers, Singapore
51. Nikhil Sud, Albright Stonebridge Group
52. Arun Mohan Sukumar, Fletcher School, Tufts University
53. John Swords, Office of Legal Affairs, NATO
54. Eneken Tikk, Cyber Policy Institute, Finland
55. Kimberley Trapp, Faculty of Laws, University College London
56. Nicholas Tsagourias, University of Sheffield
57. Antonios Tzanakopoulos, Law Faculty, University of Oxford
58. Priya Urs, ELAC, Blavatnik School of Government, University of Oxford
59. Tsvetelina van Benthem, ELAC, Blavatnik School of Government, University of Oxford
60. Larissa van den Herik, Grotius Centre for International Legal Studies, Leiden University
61. George W, GCHQ
62. Marguerite Walter, US Department of State
63. Eliza Watt, Middlesex University
64. Louis Williams, ICRC
65. Elizabeth Wilmshurst, Chatham House
66. Robert Young, Global Affairs Canada

Procedural requirements associated with the taking of countermeasures against malicious cyber operations

*Dr Przemysław Roguski**

*Lecturer in Law, Jagiellonian University in Kraków

I. Introduction

This input paper explores the procedural requirements associated with the taking of countermeasures against malicious cyber operations. Under general international law, countermeasures are "measures that would otherwise be contrary to the international obligations of an injured State vis-à-vis the responsible State, if they were not taken by the former in response to an internationally wrongful act by the latter in order to procure cessation and reparation."[1] They are measures of self-help which, in a decentralized system of law, are employed (primarily) by the injured State to vindicate its rights. Because countermeasures "justify" breaches of international law and may thus be liable to abuse, the taking of countermeasures is subject to specific conditions and limitations, in light of their exceptional character.

The United Nations Group of Governmental Experts (GGE) confirmed already in its 2013 report that "international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment."[2] The 2015[3] and 2021[4] reports further specified that "States must meet their international obligations regarding internationally wrongful acts attributable to them under international law". While neither of the reports specifically refers to countermeasures, and the 2016-2017 GGE did not produce a report because it could not find consensus on a range of issues, including the law of State responsibility,[5] most States and experts confirm that the

1 International Law Commission (ILC), Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), Commentary, Chapter II, para. 1
2 GGE Report 2013, UN Doc. A/68/98, para. 19
3 GGE Report 2015, UN Doc. A/70/174, para. 28(f)
4 GGE Report 2021, UN Doc. A/76/135, para. 71(g)
5 See Michelle Markoff, Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the

applicability of international law to cyber operations necessarily includes all rules relating to State responsibility, including countermeasures.[6]

Out of all national statements on the applicability of international law to cyber operations surveyed by the author, only China seems to question not only the applicability of the law on state responsibility to States' use of ICTs, but its binding character in general.[7] Others, such as Brazil, put into question only parts of the rules on State responsibility as laid down by the International Law Commission.[8] It has to be stressed that these positions are a clear minority and there is a substantial agreement as to the general applicability of the law of State responsibility, including countermeasures, to cyber operations.

II. Procedural requirements under the Articles on State Responsibility

The ILC's Articles on State Responsibility list two main procedural conditions relating to resort to countermeasures (Art. 52 ARSIWA):

> 1. Before taking countermeasures, an injured State shall:
> (a) call upon the responsible State, in accordance with article 43, to fulfil its obligations under Part Two;
>
> (b) notify the responsible State of any decision to take countermeasures and offer to negotiate with that State.

Furthermore, they allow the injured State to depart from the obligation of notification and offer to negotiate in cases of urgency:

Context of International Security, Remarks of 23 June 2017, online: https://2017-2021.state.gov/explanation-of-position-at-the-conclusion-of-the-2016-2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-sec/index.html [03.05.2022]

6 See e.g. Michael Schmitt, Liis Vihul (eds.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge 2017, Rule 20, p. 111

7 China's Contribution to the Initial Pre-Draft of OEWG Report, undated, online: https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf [.03.05.2022]: "And when it comes to state responsibility, which, unlike the law of armed conflicts or human rights, has not yet gained international consensus, there is no legal basis at all for any discussion on its application in cyberspace" at p. 5

8 Brazil's national contribution, UN Doc. A/76/136, p. 21: "On the other hand, there are questions on the customary status of other set of articles on state responsibility emanated from the ILC, such as the ones on countermeasures."

2. Notwithstanding paragraph 1 (b), the injured State may take such **urgent** countermeasures as are necessary to preserve its rights.

1. Sommation

The first requirement, also called sommation, obliges the injured State first call "upon the State committing the wrongful act to discontinue its wrongful conduct or to make reparation for it"[9], before instituting countermeasures. The requirement of sommation is well established in general international law[10] and has been confirmed in various cases before international courts and tribunals (*Naulilaa*,[11] *Gabcikovo-Nagymaros*[12]). The purpose of this requirement is to give the responsible State an opportunity to review its actions, alleged to be unlawful, and to either provide a justification or cease the offending action and make appropriate reparation.[13] Furthermore, it is to safeguard against an unlawful and premature resort to countermeasures.[14]

2. Notification and offer to negotiate

The second procedural requirement – notification of the intent to take countermeasures, paired with an offer to negotiate – has a more troubled drafting history. Earlier versions of what is now Article 52 allowed the resort to unilateral action only after all options of amicable dispute settlement been exhausted. While this requirement has not been reflected in the abovementioned decisions of international tribunals which formed the basis for the ILC's codification attempts, the ILC has extensively discussed the necessity of prior dispute settlement as a consequence of article 33(1) UN Charter, whereby "[t]he parties to any dispute [shall], first of all, [my own underlining – PR] seek a solution

9 Gabcikovo-Nagymaros case, ICJ Rep. 1997, 7, para. 84

10 For an overview and discussion see Gaetano Arangio-Ruiz, Fourth Report on State Responsibility, ILC Yearbook 1992, Vol II(1), 1, 22, paras. 6ff.

11 „La représaille est un acte de propre justice (Selbsthilfehandlung) de l'État lésé, acte répondant — après sommation restée infructueuse — à un acte contraire au droit des gens de l'État offenseur", Naulilaa case, RIAA 1928, Vol. II, p. 1026

12 Gabcikovo-Nagymaros case, ICJ Rep. 1997, 7, para. 84

13 Yuji Iwasawa, Naoki Iwatsuki, Chapter 81 – Procedural Conditions, [in:] James Crawford et al. (eds.), The Law of International Responsibility, OUP 2010, p. 1151.

14 Report of the International Law Commission on the work of its forty-fourth session, UN Doc. A/47/10, para. 172

by negotiation, enquiry (...)" etc. Acknowledging the uncertainties surrounding the existing practice, special rapporteur Arangio-Ruiz has nevertheless argued that, based on the UN Charter and some examples of practice, it would be advisable to include a provision whereby "an injured State must refrain from unilateral measures that may jeopardize an amicable solution until it becomes clear that the means of settlement, other than negotiation, at the disposal of the parties have failed to bring about or are unlikely to bring about any concrete result.[15]

The requirement of prior recourse to dispute settlement procedures has proven very controversial among the ILC members and the next special rapporteur, James Crawford, shared the firm view that the linkage between countermeasures and dispute settlement was unworkable and thus unsustainable.[16] This requirement has thus ultimately been abandoned[17] in favour of a proposal by Bennouna whereby "Prior to taking countermeasures, an injured State shall fulfil its obligation to negotiate" (the proposal was narrowly adopted by 13 to 9 votes).[18] But the subsequent draft, which included Bennouna's proposal to impose on the injured State an obligation to negotiate, has also led to much controversy and a heated debate among States in the UNGA Sixth Committee, which Crawford summed up as follows "On the one hand, Governments continue to express concern at the possibility of unilateral determinations on the part of the State taking countermeasures. On the other hand, the procedural conditions laid down in article 53 [as it then was] have been strongly criticized as unfounded in international

15 Gaetano Arangio-Ruiz, Fourth Report on State Responsibility, ILC Yearbook 1992, Vol II(1), 1, 22, para. 41

16 Report of the International Law Commission on the work of its fifty-first session, A/CN.4/SER.A/1999/Add.I, para. 436

17 For a discussion of the reasons see Gaetano Arangio-Ruiz, Sixth Report on State Responsibility, ILC Yearbook 1994, Vol II(1), 1, paras. 6ff.

18 ILC, Summary record of the 2456th meeting, UN Doc. A/CN.4/SR.2456, para. 57. The reasons for such a provision were cited by Bennouna as "first, it was directly in line with Article 33 of the Charter of the United Nations; secondly, it enabled the parties, regardless of the outcome of the negotiations, to exchange views and clearly state their respective positions; thirdly, it would discourage powerful countries from being tempted to take advantage of their dominant position; and, fourthly, it offered the parties a practical and realistic solution, for, as Mr. Pellet had pointed out, arbitration could go on for years.", ibidem. para. 33. Opponents such as Villagrán Kramer argued that there was not „one single example among the cases cited by the former Special Rapporteur showing that such an obligation existed.", ibidem. para. 44.

law and as unduly cumbersome and restrictive. For the opponents of countermeasures, article 53 does not do enough; for their proponents, it goes much too far (footnotes omitted – PR)."[19] Ultimately, the final draft dropped the "obligation to negotiate" in favour of a less restrictive "offer to negotiate", taking into account the fact that an obligation to negotiate may be difficult to discharge if the responsible State does not want to participate in such negotiations and thus the injured State's right to institute countermeasures would be subject to the responsible State's cooperation.

3. Urgent countermeasures

Art. 52(2) ARSIWA allows the injured State to take "such urgent countermeasures as are necessary to preserve its rights." The "preservation of rights" includes both the rights affected by the internationally wrongful act of the responsible State and the injured State's right to take countermeasures.[20] Urgent action my become necessary especially when the responsible State may seek to immunize itself from countermeasures and thus the injured State must act speedily and with surprise to be able to achieve the intended effect of its countermeasures. To this effect, the injured State may dispense with the requirement to notify the responsible State of its intention to take countermeasures. Crucially, though, paragraph 2 makes it clear that the 'urgency exception' applies only to the requirement of notification and offer to negotiate, not to the requirement of *sommation.*

The formulation of Art. 52(2) ARSIWA is again the product of a compromise between differing positions within the ILC. Prior drafts included a distinction between "provisional countermeasures" and countermeasures proper, which could only be imposed after all other measures of dispute resolution were unsuccessful. This distinction was ultimately dropped in favour of the current formulation, also to underline the fact that all countermeasures are in their essence provisional and must be stopped once the responsible State ceases its wrongful act.

19 James Crawford, Fourth Report on State Responsibility, UN Doc. A/CN.4/517 and Add.1, para. 67
20 ILC ARSIWA Commentary, Art. 52, para. 6

It bears recalling that there is also some debate as to whether the regulation of urgent countermeasures by the ILC reflected existing international law, or constituted its progressive development. Special rapporteur Crawford, for instance argued that "the distinction between urgent and definitive countermeasures does not correspond with existing international law."[21]

III. Procedural requirements in national contributions on how international law applies to cyber operations

So far, no less than 17 States have addressed the applicability of the law of countermeasures to cyber operations. Out of these, only Brazil voices its reservation to the general applicability of countermeasures, stressing the need for further discussion as there are "many factors advising a cautious approach to countermeasures."[22] Six States specifically address (some of) the procedural conditions associated with the taking of countermeasures. From these statements, a few crucial observations on the challenges attached to the application of the procedural conditions for the taking of countermeasures (as laid down in the Articles on State Responsibility) can be made.

1. Sommation and Notification – one or two requirements?

First, it has to be noted that many States do not clearly distinguish between the requirements of *sommation* (Art. 52(1)(a) ARSIWA) and the requirement of notification and offer to negotiate (Art. 52(1)(b)

21 James Crawford, Fourth Report on State Responsibility, UN Doc. A/CN.4/517 and Add.1, para. 69: "But it must be conceded at once that the distinction between urgent and definitive countermeasures does not correspond with existing international law. It was developed in the course of the first reading by way of a compromise between sharply opposed positions on the suspensive effect of negotiations. The distinction is more a guide to the application of principles of necessity and proportionality in the given case than it is a distinct requirement."

22 Brazil's national contribution, UN Doc. A/76/136, p. 22: "First, there is an added difficulty to attribute cyber activities to a particular State, which is aggravated by the fact that States have different technical resources and capabilities to both identify the origins of a cyber activity and to verify claims of breaches of international obligations through cyber means. Second, cyber operations can be designed to mask or spoof the perpetrator, which in turns increase the risks of miscalculated responses against innocent actors. Finally, the speed with which the precipitating wrongful cyber operations may unfold poses a high risk of escalation, with potential rippling effects to the kinetic domain."

ARSIWA). Only Italy[23] and Norway[24] make this distinction clear in their statements. Other States seem to omit either the requirement of sommation or that of notification. For instance, the United States in its 2016[25] and 2021[26] statements refer to the requirement of "prior demand", which it equates with sommation:

> "[An injured State] generally must call upon the responsible State to cease its wrongful conduct, unless urgent countermeasures are necessary to preserve the injured State's rights." [27]

On the other hand, Israel[28] and the Netherlands[29] speak only of an obligation of "prior notification", without distinguishing between sommation and notification proper.

This may be due to the fact that Art. 52 ARSIWA does not require any specific sequencing between sommation and notification and in practice both requirements can be fulfilled at the same time and through the same act,[30] thus leading some States to combine both elements. This seems to be the position of the United Kingdom, which states:

> "The UK does not consider that States taking countermeasures are legally obliged to give prior notice (including by calling on the State responsible for the internationally wrongful act to comply with international law) in all circumstances."[31]

23 Italian Position Paper on 'International Law and Cyberspace', online: https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf [03.05.2021], p. 7: "[the] victim-State is generally required to call upon the State of origin to discontinue the wrongful act and to notify it of its intention to take countermeasures in response to wrongful cyber operations."
24 Norway national contribution, UN Doc. A/76/136, p. 73: "The State held responsible should be notified of both the violation of international law and the grounds for attribution, as well as of the intention to introduce countermeasures."
25 Brian J. Egan, International Law and Stability in Cyberspace, 35 Berkeley J of Int'l Law 169 (2017), p. 178
26 United States national contribution, UN Doc. A/76/136, p. 142
27 Ibidem.
28 Roy Schondorf, Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations, 97 Int'l L Studies 395 (2021), p. 405
29 Netherlands national contribution, UN Doc. A/76/136, p. 63
30 ILC ARSIWA Commentary, Art. 52, para. 5
31 UK national position, UN Doc. A/76/136, p. 118

While there may be good arguments to calling upon the responsible State to fulfil its obligations and to notifying it of the intent to take countermeasures in one act, both conditions need to be clearly distinguished with regard to the taking of urgent countermeasures.

2. Is 'prior demand' necessary when responding to cyber operations?
Some States, in particular Israel, the United Kingdom and the United States, argue that a 'prior demand' is not necessary when responding to cyber operations, either generally or at least in specific circumstances. Out of these three, the United States takes the most cautious position, arguing that:

> The sufficiency of this prior demand on the responsible State should be evaluated on a case-by-case basis in light of the particular circumstances of the situation at hand and the purpose of the requirement, which is to give the responsible State notice of the injured State's claim and an opportunity to respond."[32]

The United Kingdom goes further, generally calling into question the applicability of a prior notification requirement to cyber situations, due to the covert nature of either the cyber intrusion or the cyber responses:

> "The UK does not consider that States taking countermeasures are legally obliged to give prior notice (including by calling on the State responsible for the internationally wrongful act to comply with international law) in all circumstances. Prior notice may not be a legal obligation when responding to covert cyber intrusion with countermeasures or when resort is had to countermeasures which themselves depend on covert cyber capabilities. In such cases, prior notice could expose highly sensitive capabilities and prejudice the very effectiveness of the countermeasures in question."[33]

Lastly, Israel agrees with the UK view that for reasons of utility and effectiveness, a requirement of prior notification may generally not be applicable to cyber operations:

32 United States national contribution, UN Doc. A/76/136, p. 142
33 UK national position, UN Doc. A/76/136, p. 118

> "With respect to the issue of countermeasures, I would like to echo the positions taken by the United Kingdom, the United States, and other States, to the effect that there is no absolute duty under international law to notify the responsible State in advance of a cyber-countermeasure. Prior notification is perhaps more realistic and practical in fields such as international trade, allowing the responsible State to reconsider its actions without frustrating the ability of the injured State to take the intended countermeasures. However, in the cyber domain, where the pace of events can be extremely fast and the other side may thwart the action if it anticipates it, announcing a cyber-countermeasure in advance would often negate its utility and effectiveness, and in some instances undermine the interests of the injured State, as well as render the countermeasure obsolete."[34]

3. When are urgent countermeasures allowed?

Lastly, some States (Italy, France, the Netherlands, Norway) affirm Art. 52 ARSIWA to the extent that in cases of urgency, a State may refrain from informing the responsible State of the intent to take countermeasures. However, for most of these States – Italy being the exception – the reasons quoted for this 'urgency exception' mostly revolve around the necessity of protecting the State's covert capabilities. For instance, France argues that:

> "the use of counter-measures requires the State responsible for the cyberattack to comply with its obligations. The victim State may, in certain circumstances, derogate from the obligation to inform the State responsible for the cyberoperation beforehand, where there is a need to protect its rights. The possibility of taking urgent counter-measures is particularly relevant in cyberspace, given the widespread use of concealment procedures and the difficulties of traceability."[35]

34 Roy Schondorf, Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations, 97 Int'l L Studies 395 (2021), p. 405

35 Ministry of Defense of France, International Law Applied to Operations in Cyberspace, 9 September 2019, p. 7-8.

Similarly, Norway argues that

> "Countermeasures may be taken without prior notification to the responsible State if providing such notification might reveal sensitive methods or capabilities or prevent the countermeasures from having the necessary effect. For example, the injured State could carry out a cyber operation to disrupt the capability of the aggressor State conducting the internationally wrongful cyber operation such as election interference. This countermeasure would in other circumstances be in violation of the aggressor State's sovereignty."[36]

IV. Summary and Assessment

The preceding analysis has shown that while there is general agreement on the applicability of the law of State responsibility to internationally wrongful acts committed by cyber means, there remains significant uncertainty and divergence of opinions with regard to the procedural conditions for the imposition of countermeasures. This uncertainty affects both the existence of any procedural conditions at all, as well as their scope.

First, Israel's and the United Kingdom's position denying the requirement to give 'prior notice' seems to be at least partially at odds with general international law as confirmed in ICJ jurisprudence. While it is debatable whether the requirement of prior notification as laid down in Art. 52(1)(b) reflected existing practice or was progressive development on the part of the ILC, no such doubts can exist with respect to the requirement of sommation, which has been confirmed in Gabcikovo-Nagymaros[37] Insofar as Israel and the United Kingdom deny the applicability of sommation (which the United Kingdom does explicitly), this would seem to go beyond the interpretation of existing international law and constitute State practice aimed at establishing a cyber-specific exception to the requirement of sommation. Of course, at this point the practice of only two States does not meet the North Sea Continental Shelf criteria for the establishment of customary international law

36 Norway national position, UN Doc. A/76/136, p. 73
37 Gabcikovo-Nagymaros case, ICJ Rep. 1997, 7, para. 84

and it remains to be seen whether other States will join this particular position. In any case, the Israel-UK position would benefit from further clarification, especially on the question whether this understanding refers to sommation as a condition for the taking of countermeasures in general or whether it is a narrower exception only with respect to cyber-countermeasures, as the Israeli position seems to suggest (with the consequence that sommation would still be necessary if non-cyber countermeasures were to be instituted against a State responsible for a wrongful cyber operation).

Secondly, even States which do not deny the existence of the sommation requirement as such, but rather argue for it being subject to the 'urgency exception' (United States and Italy) would need to clarify why States may dispense with both sommation and notification in cases of urgent countermeasures, where Art. 52(2) ARSIWA specifically exempts urgent countermeasures only from the requirement of notification. Given that countermeasures, as envisaged by the ILC, are measures of last resort against "a State which is responsible for an internationally wrongful act and which refuses to cease that act or provide any redress",[38] it seems indispensable that such a State be first informed of the claim the injured State has against it.

The author acknowledges that there may be significant policy arguments for dispensing with the requirement of notification and possibly even sommation, at least in cases of urgent countermeasures. It needs to be kept in mind that in many situations where a State is faced with an ongoing cyber operation, even a reliable legal attribution may be difficult without extensive cyber-forensic work, whereas the urgency of stopping the cyber operation would dictate the need to take countermeasures against the source of the attack, even prior to forensic work being concluded.[39] Nevertheless, especially where those policy arguments

38 ILC ARSIWA Commentary, Article 52, para. 6

39 See to this effect the Finnish position, which argues that "Some of the procedural requirements concerning countermeasures may nevertheless require adjustment. For instance, it may be possible to attribute a hostile cyber operation only afterward whereas countermeasures normally should be taken while the wrongful act is ongoing.", International law and cyberspace - Finland's national positions, online:

go against general international law as confirmed in the jurisprudence of international tribunals, further clarification by States and analysis by scholars seems necessary and advisable.

In conclusion, it seems Canada was right when it stated that

> "[t]he precise scope of certain procedural aspects of countermeasures, such as notification, needs to be further defined through State practice given the unique nature of cyberspace."[40]

https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af-3c6d85?t=1603097522727 [03.05.2022]

40 Government of Canada, International Law applicable in cyberspace, online: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng [03.05.2022], para. 24

Collective Countermeasures in Cyberspace

*Lori F. Damrosch**

12 May 2022

*Hamilton Fish Professor of International Law and Diplomacy, Columbia Law School

I Terminology and Concepts

A. Collective Countermeasures

The term "collective countermeasures" in the panel's title is found in international legal scholarship,[1] but it does not have an authoritative definition in a legal instrument. Following the Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA, or the Articles) adopted by the UN International Law Commission (ILC) in 2001,[2] countermeasures consist of an otherwise unlawful (wrongful) act that is rendered lawful (its wrongfulness is precluded) because it responds to a prior unlawful (wrongful) act. However, while the ILC's treatment is a natural starting point, it neither answers the core question of the lawfulness of collective countermeasures – in general, or in cyberspace in particular – nor, if it purported to do so, would it foreclose states from taking a different approach. As David Caron wisely observed, ARSIWA's rule-like formulations do not necessarily enjoy the same authority or legal quality as, say, the Vienna Convention on the Law of Treaties:[3] some of the ILC's choices – notably those on countermeasures – were controversial, involved elements of compromise, and in many respects clearly

1 Scholarly references include Michael N. Schmitt & Sean Watts, Collective Cyber Countermeasures? 12 Harv. Nat. Sec. J. 373 (2021); Jeff Kosseff, Collective Countermeasures in Cyberspace, 10 Notre Dame J. Int'l Comp. L. 18 (2020); Przemyslaw Roguski, Collective Countermeasures in Cyberspace – Lex Lata, Progressive Development or a Bad Idea? in 20/20 Vision: The Next Decade 25 (T. Jancarova et al., 2020); Samuli Haataja, Cyber Operations and Collective Countermeasures under International Law, 25 J. Conflict & Sec. L. 33 (2020). Other terms include "third- party countermeasures." See Martin Dawidowicz, Third-Party Countermeasures in International Law (2017); see also Elena Katselli Proukaki, The Problem of Enforcement in International Law: Countermeasures, the Non-Injured States and the Idea of International Community (2010).

2 UN International Law Commission, Articles on Responsibility of States for Internationally Wrongful Acts, UN Doc. A/56/10 (2001), Arts. 22, 49-54.

3 See David D. Caron, The ILC Articles on State Responsibility: The Paradoxical Relationship Between Form and Authority, 96 AJIL 857 (2002). See also David J. Bederman, Counterintuiting Countermeasures, 96 AJIL 817 (2002).

constituted progressive development rather than codification of the law.

"Collective" as an adjective modifying countermeasures is not self-defining and can be confusing. Under one reading, it suggests an analogy to collective self-defense: that is, lawful third-party responses to an unlawful armed attack for collective self-defense, and lawful third- party responses to a broader category of forcible or nonforcible breaches for collective nonforcible countermeasures.[4] An analogy to collective self-defense for collective countermeasures could bring into play a repertoire of criteria drawn from international case law on armed activities, such as requirements that a state whose individual rights are at stake have declared itself to have been attacked (injured); that it have requested other states to come to its aid; that third states responding to such a call for assistance remain within the bounds of what the attacked (injured) state desires by way of outside help; and that third-state assistance comply with requirements applicable to the attacked (injured) state itself, such as necessity or proportionality.[5]

Under another reading, collective countermeasures would be analogous to collective security – lawful measures which the UN Security Council may authorize not only in response to unlawful armed attacks, but also in respect of threats to or breaches of peace.[6] If a permanent member's veto blocks the Council from adopting compulsory measures in response to such a threat that also involves breach of an international obligation, collective countermeasures could help fill the enforcement gap. A blocking veto would prevent the measures from

4 UN Charter, Art. 51 (inherent right of individual or collective self-defense).
5 On such criteria in the context of collective self-defense, see Military and Paramilitary Activities in and Against Nicaragua, 1986 ICJ 14, 103-123. To the extent that the Court appeared to restrict justifiable countermeasures to "victim" states – El Salvador, Honduras, or Costa Rica – and to foreclose a third state, the United States, from taking such measures, the passage in question emphasizes its particular application to intervention involving the use of force (p. 127, para. 249). Elsewhere, the Nicaragua decision also addressed certain nonforcible measures, such as the U.S. reduction of sugar imports from Nicaragua in relation to the customary international law of nonintervention and a bilateral treaty (pp. 126, 138, paras. 245, 276). Collective (third-party) nonforcible countermeasures are not clearly addressed under the then-evolving law of state responsibility, nor resolved in a way that would preclude fresh examination.
6 UN Charter, Chapter VII, Art. 39. Such threats might, but need not, involve violations of international law.

becoming compulsory on all UN members; but a theory of collective countermeasures would authorize states to apply sanctions to induce an end to the breach. Nonforcible collective countermeasures could be comparable to measures available to the Council under Article 41 of the Charter – "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations."

Analogizing collective countermeasures to collective self-defense or collective security could be problematic, in view of the fact that the law applicable to each involves conditions developed to constrain forcible responses to forcible acts (or at least peace-threatening ones). Our focus here – like the ILC's treatment of countermeasures – is nonforcible responses to violations of international law; armed reprisals are excluded.[7] However, the predicate violations for nonforcible countermeasures could entail forcible conduct, such as unlawful resort to armed force (jus ad bellum) or unlawful conduct in an armed conflict (jus in bello). I do not address limitations specific to the laws of armed conflict (LOAC) on suspending performance of obligations under LOAC in response to violations committed by others.[8]

B. Collective Countermeasures in Cyberspace Should Be Lawful in Principle

In a valuable recent article, Michael Schmitt and Sean Watts review the arguments for and against collective countermeasures and conclude that although the issue remains unsettled, collective cyber countermeasures in support of injured states are lawful.[9] I agree. The issues are indeed difficult – so difficult that Professor Schmitt acknowledges having changed his mind from an earlier view that collective countermeasures are impermissible, to a view that evolved in light of the changing threat environment and seven years of discussions

7 Cf. Lori Fisler Damrosch, Enforcing International Law Through Non-Forcible Measures, 269 Rec. des Cours 9 (1997), pp. 45-46 (on collective economic sanctions), 52-61 (on the ILC's treatment of countermeasures as of 1997, shortly before the completion of ARSIWA in 2001).
8 Cf. ARSIWA, Art. 50(1)(c), on obligations of a humanitarian character prohibiting reprisals.
9 Schmitt & Watts, supra.

with government policy-makers in many countries.[10] A permissive view of collective cyber countermeasures would enable smaller states to seek the aid of stronger states, or those with stronger cyber resources, in order to enforce violations that would otherwise go unremedied. I find those arguments quite persuasive, on grounds of both policy and law. Although some authors doubt that collective countermeasures have had or would have much effect in inducing violator states to comply with their obligations,[11] reversing an ongoing illegal course of conduct is not the only purpose that collective countermeasures can serve. Equally important is the expressive function of affirming collective commitment to the primary rules at stake, and signaling that future violations – by the current violator, or by other potential violators bound to the same obligations – will incur predictable and proportionate costs.[12]

C. Distinctions: Erga Omnes, Jus Cogens, and "Serious" Violations

This workshop's theme statement crystallizes a controversy over the lawfulness of countermeasures taken by a state that is "not directly injured" by the breach and invites us to consider whether only breaches of obligations owed erga omnes qualify as lawful collective countermeasures. This framing tracks the ILC's assumption that in general only an "injured state" may invoke the responsibility of another state and apply countermeasures against it,[13] and that a state other than an injured state may do so only in respect of a group's collective interests, or when the breach is of an obligation "owed to the international community as a whole."[14]

We can analyze obligations and breaches by asking three questions: (1) To whom is the obligation owed? (2) Is it hierarchically superior to other

10 Id. at 373 n. *.
11 See Christian J. Tams, Enforcing Obligations Erga Omnes in International Law 229 (2d. ed. 2010).
12 See Monica Hakimi, Constructing an International Community, 111 AJIL 317, 349 (2017) (significance of third- party countermeasures as "an occasion for multiple states to rally behind the violated norms and to insist that these norms apply equally to all states").
13 On invocation of responsibility by an injured state, see ARSIWA, Arts. 42-47; and on the application of countermeasures by an injured state, see ARSIWA, Art. 49.
14 ARSIWA, Art. 48, quoted more fully and discussed below.

obligations? (3) Is the breach serious?

1. To whom is the obligation owed? To one state only; to several states; or to all states?[15]

In Barcelona Traction, the ICJ alluded to a category of obligations owed "towards the international community as a whole," which by their very nature "are the concern of all States. In view of the importance of the rights involved, all States can be held to have a legal interest in their protection; they are obligations erga omnes." The Court suggested the following examples of such obligations: "the outlawing of acts of aggression, and of genocide, as also from the principles and rules concerning the basic rights of the human person, including protection from slavery and racial discrimination."[16] Evidently, this was and is not a closed list, nor is the overlapping but analytically distinct category of peremptory norms (jus cogens) discussed next.

Additionally, the vocabulary of erga omnes partes enables consideration of the legal interests of the states that are parties to a treaty establishing primary rules of conduct, whether or not those primary obligations are owed to "the international community as a whole." The case brought by The Gambia against Myanmar under the Genocide Convention involves an obligation from Barcelona Traction's erga omnes short list; the procedural issues now being litigated include the particular legal interests of treaty parties to invoke treaty-based dispute settlement.[17]

15 ARSIWA, Art. 48(1) provides that any state is entitled to invoke the responsibility of another state if:
(a) The obligation breached is owed to a group of States including that State, and is established for the protection of a collective interest of the group; or
(b) The obligation breached is owed to the international community as a whole.
The ILC commentary illustrates the "collective obligations" of paragraph 1(a) with examples including environmental protection, regional security (such as a nuclear free zone treaty) or regional human rights systems. UN Doc. A/56/10, at 320-321 (2001). For critique of the concept of "international community" under ARSIWA's assumptions about obligation erga omnes, see Hakimi, supra, at 335-337.
16 Barcelona Traction, Light and Power Company, Ltd. (Belgium v. Spain), 1970 ICJ 3, paras. 33-34.
17 Application of the Convention on the Prevention and Punishment of the Crime of Genocide (The Gambia v. Myanmar), 2020 ICJ (Order on Request for the Indication of Provisional Measures), para. 41 ("It follows that any State party to the Genocide Convention, and not only a specially affected State, may invoke the responsibility of another State party with a view to ascertaining the alleged failure to comply with its obligations erga omnes partes, and to bring that failure to an end."). See also Questions relating to the Obligation to Prosecute or Extradite (Belgium v. Spain), 2012 ICJ 449, para. 68 (Convention against Torture

2. Is the obligation hierarchically superior to other obligations?
In other words, does it enjoy the status of a peremptory norm (jus cogens), with all the legal consequences attaching to that status?[18] Articles 53 and 64 of the Vienna Convention on the Law of Treaties invalidate treaties conflicting with such norms. The ILC commentary on the Vienna Convention suggests the following non-exclusive examples of peremptory norms:

> (a) a treaty contemplating an unlawful use of force; (b) a treaty contemplating performance of any other act criminal under international law; and (c) a treaty contemplating the commission of acts, such as the slave trade, piracy, or genocide, "in the suppression of which every State is called upon to cooperate."

The commentary continues that other possible examples could include "treaties violating human rights, the equality of States or the principle of self-determination."[19]

ARSIWA expands the consequences of violations of peremptory norms to include requirements of cooperation in suppression, non-recognition, and prohibitions on rendering assistance in maintaining violations, at least where the breach is "serious."[20]

In 2015, the ILC returned to the study of peremptory norms. The most recent report of its Special Rapporteur, Dire Tladi (January 2022), offers the following "non-exhaustive list":.[21]

---

generates obligations erga omnes partes "in the sense that each State party has an interest in compliance with them in any given case").
18 See ARSIWA, Arts. 40-41 on "Serious breaches of obligations under peremptory norms of general international law."
19 [1966] II Y.B.I.L.C. 169, 247-249, para. (3).
20 See ARSIWA, Art. 41 "Particular consequences of a serious breach of an obligation under this chapter." Article 40 states that a breach of such an obligation is serious "if it involves a gross or systematic failure by the responsible State to fulfil the obligation." See infra, sec. C.3. See also ARSIWA, Art. 26 on compliance with peremptory norms; Art. 50(1)(d) (countermeasures shall not affect obligations to comply with peremptory norms).
21 Fifth Report on Peremptory Norms of General International Law (Jus Cogens) by Dire Tladi, Special Rapporteur, UN Doc. A/CN.4/747 (Jan. 24, 2022), pp. 66-69, 82-83, Conclusion 23 ("Non-exhaustive list") and Annex.

(a) The prohibition of aggression;
(b) The prohibition of genocide;
(c) The prohibition of crimes against humanity;
(d) The basic rules of international humanitarian law;
(e) The prohibition of racial discrimination and apartheid;
(f) The prohibition of slavery;
(g) The prohibition of torture;
(h) The right of self-determination.

3. How serious is the violation in the instance at hand?

As noted above, ARSIWA singles out "serious" breaches of peremptory norms for special consequences entailing not only rights and permissions, but potentially even duties for every state.[22] Subject to concerns previously noted about uncritical assumptions that every aspect of ARSIWA enjoys the same normativity as treaty-based or customary international law, there may be a basis within the Articles for considering that at least those violations involving "gross or systematic failure" to fulfill obligations under peremptory norms entail the consequence of at least authorizing, if not requiring, states to "cooperate to bring to an end through lawful means any serious breach" of such an obligation.[23] Collective countermeasures, under the view endorsed here, should be considered "lawful means" of cooperation in this sense.

II. Examples of Collective Countermeasures

I will illustrate the problem of collective countermeasures with several examples drawn from prior or current situations of actual or potential collective responses to a state's violation of international obligations. Such examples could well, but need not, involve violations committed by way of cyberattacks, and/or countermeasures in cyberspace. The first example is taken from actual events concerning individual and collective

22 Compare other international regimes requiring attention to the seriousness or gravity of a breach, e.g. "grave breaches" under the Geneva Conventions or "gravity" under the Rome Statute of the International Criminal Court.
23 ARSIWA, Art. 41(1).

economic sanctions against violations of diplomatic and consular law. The second and third examples concern countermeasures against violations of obligations under nonproliferation and antiterrorism regimes.

A. Obligations Involving Diplomatic or Consular Law

The paradigmatic example of countermeasures to violations of diplomatic and consular law is the Tehran hostage crisis of 1979-1981. Student militants, soon backed by the highest authorities of the Islamic Republic of Iran, captured the premises and personnel of the U.S. embassy in Tehran and held more than 50 members of the diplomatic and consular staff hostage for 444 days. Within the first weeks of the crisis and in several waves thereafter, the United States first applied individual countermeasures and later sought collective support through the UN Security Council, which initially signaled support for the United States but never adopted Chapter VII sanctions due to a Soviet veto.[24] Meanwhile, relying on several treaties with compromissory clauses providing for dispute settlement at the International Court of Justice, the United States brought an application to the ICJ and obtained both a provisional measures order and a final merits judgment. The latter judgment deals obliquely with the U.S. countermeasures, implicitly approving them in a passage indicating the majority's disagreement with the view of Soviet Judge Morozov that the U.S. economic sanctions may have been unlawful or that U.S. resort to self-help may have disqualified it from judicial relief.[25] The ICJ's opinion was one of the first international decisions addressing countermeasures and figured in the ILC's examination of related issues in its study of state responsibility.

Another aspect of the Tehran hostage crisis – less well known than the ICJ case, but relevant to our workshop's consideration of collective countermeasures – was the U.S. effort to enlist states in which Iran

24 On the veto, see 80 Dep't State Bull. No. 2035, at 67-71 (Feb. 1980).
25 United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), 1980 ICJ 3, 27-28 (referring to U.S. sanctions as countermeasures "taken in response to what the United States believed to be grave and manifest violations of international law by Iran"); 1980 ICJ 51, 53-55 (Morozov, J., dissenting in part).

had significant economic interests to join in denying Iran the benefits of normal economic and financial relations for as long as Iran continued its illegal activity of holding diplomatic and consular hostages. After the Soviet veto of compulsory UN sanctions, the United States persuaded its allies to apply some of the same economic sanctions that were proposed in the U.S. draft Security Council resolution, in order to strengthen the economic pressure on Iran to induce it to release the hostages.[26] The U.S. arguments in favor of multilateral economic sanctions relied in part on the proposition that not only the United States, but all states, had a collective interest in enforcing the obligations of host states under diplomatic and consular law – in other words, an argument in favor of collective countermeasures.

In its 1980 Tehran Hostages judgment, the ICJ considered it to be its duty to draw the attention of the entire international community, of which Iran itself has been a member since time immemorial, to the irreparable harm that may be caused by events of the kind now before the Court. Such events cannot fail to undermine the edifice of law carefully constructed by mankind over a period of centuries, the maintenance of which is vital for the security and well-being of the complex international community of the present day, to which it is more essential than ever that the rules developed to ensure the ordered progress of relations between its members should be constantly and scrupulously respected.[27]

The Court's references to the interest of "the entire international community" in the regime of diplomatic law are suggestive of erga omnes obligations and could imply support for the view that countermeasures by states not directly injured by the violation would be lawful. However, neither the ICJ, nor the ILC in ARSIWA or its commentary, has clearly endorsed collective countermeasures for

26 On the U.S. effort to multilateralize the economic sanctions in the aftermath of the Soviet veto of the Chapter VII resolution, see 80 Dep't State Bull. No. 2039, at 49 (June 1980); see also 80 Dep't State Bull. No. 2040, at 71-73
(July 1980).
27 1980 ICJ 43.

violations of diplomatic or consular law, which in other respects are treated as self-enforcing under "self-contained regimes" operating on the basis of reciprocity.[28]

Although cyber technology was only in its infancy in 1979-1981, the Tehran hostage crisis readily illustrates the need for lawful measures of collective response in situations that could well entail cyber elements. Embassy premises can be both platforms for, and targets of, cyberattacks. Diplomatic and consular personnel, who enjoy immunity and inviolability under the treaty-based regimes and parallel customary international law, can be both perpetrators and victims of cyberattacks. Diplomatic and consular communications are likewise legally protected and supposed to be inviolable, yet cyber intrusions are commonplace. Especially where smaller states would otherwise be unable to apply meaningful sanctions against violators, collective countermeasures may be the only available tools for enforcement of diplomatic and consular law.

B. Nonproliferation of Weapons of Mass Destruction

The regime of nuclear nonproliferation law centers on the Treaty on the Non- Proliferation of Nuclear Weapons (NPT), to which the vast majority of states are parties.[29] However, because the NPT establishes two different sets of obligations applicable, respectively, to nuclear-weapons states (NWS) and non-nuclear-weapons states (NNWS), its provisions would not qualify for customary international law status under the usual criteria for treaty provisions giving rise to "a general rule of law."[30] Moreover, several important nuclear-capable powers are not

28 1980 ICJ 40 ("self-contained regime" of diplomatic law has its own remedies for breach). Cf. Bruno Simma & Dirk Pulkowski, Of Planets and the Universe: Self-contained Regimes and International Law, 17 EJIL 483 (2006) ("self-contained regimes" presuppose the operation of general rules of state responsibility). ARSIWA Art. 50(2)(b) requires states taking countermeasures to "respect the inviolability of diplomatic or consular premises, archives and documents," without explicitly stating that violations of those obligations can justify collective countermeasures.

29 Treaty on the Non-Proliferation of Nuclear Weapons, done at London, Moscow and Washington, July 1, 1968, 729 UNTS 161.

30 North Sea Continental Shelf (FRG v. Denmark; FRG v. Netherlands), 1969 ICJ 3, paras. 72-75 (to generate customary international law, a treaty provision should "be of a fundamentally norm-creating character such as could be regarded as forming the basis of a general rule of law," considering also the practice of

only not parties to the NPT, but have denied the existence of customary international law rules constraining them from nuclear activities. Several of them, notoriously, have acted contrary to the constraints applicable to NPT parties, through nuclear activities up to and including the testing of nuclear explosive devices. It would thus seem implausible to qualify obligations of nuclear nonproliferation as owed "to the international community as a whole" under ARSIWA.

Security Council practice under Chapter VII of the UN Charter has included several programs of compulsory sanctions against NNWS who appeared to be out of compliance with obligations under the NPT and related safeguards regimes administered by the International Atomic Energy Agency. In situations involving Iraq for much of the period between 1990 and 2003, the Democratic People's Republic of Korea from 2006 onward, and Iran from 2006 until implementation of the 2015 Joint Comprehensive Plan of Action, the Security Council has required all UN members to restrict their economic and other relations with the targets to induce them to comply with their nonproliferation obligations. The United States and some other states have applied more stringent measures of economic denial than those mandated by the Security Council's Chapter VII resolutions on nonproliferation.

In situations involving probable, even provable, violations of NPT obligations, in which the Security Council might be blocked from applying sanctions due to a permanent member veto, ARSIWA's provisions offer imperfect guidance on evaluating collective efforts to impose economic restrictions that might place the sanctioning states in violation of obligations owed to the targets. Although the future of the planet may depend on NPT compliance, the two-tiered nature of NPT obligations makes an uncomfortable fit with traditional conceptions of erga omnes or jus cogens obligations; erga omnes partes arguments, while plausible in respect of NPT violations, seem unduly technical given the stakes. A flexible conception of collective countermeasures would be preferable.

specially affected states).

Other regimes for control of weapons of mass destructions, such as treaties prohibiting biological or chemical weapons, should be considered along similar lines. However, since their prohibitions are general rather than two-tiered, and almost universally followed, the argument for countermeasures on behalf of "the international community as a whole" is easier to make.

Collective countermeasures against violations of WMD obligations could well entail cyber operations, since nuclear enrichment and other relevant technologies rely heavily on cyber systems.

C. Terrorism

Apart from the several sanctions regimes applied by the UN Security Council against state or non-state actors involved in certain kinds of terrorist activities,[31] some states have imposed their own economic sanctions on state sponsors of terrorism. For many years, the United States has listed Iran as a state sponsor of terrorism and maintained a wide range of antiterrorism sanctions against it. Among other tools, U.S. legislation has lifted Iran's sovereign immunity that would otherwise have protected it from suit, attachment, and execution under the Foreign Sovereign Immunities Act (FSIA); and the U.S. Supreme Court rejected Iran's challenge to FSIA amendments allowing plaintiffs holding judgments against Iran amounting to hundreds of millions of dollars to levy against assets of the Iranian central bank held in the United States.[32] Thereafter, Iran sued the United States at the ICJ, invoking a 1955 Treaty of Amity, Economic Relations, and Consular Rights, which Iran says the United States violated in allowing seizure of Iranian assets.[33] After a decision partially upholding and partially rejecting U.S. preliminary objections, briefing on the merits is now in progress.

31 E.g., sanctions against Libya for its involvement in the terrorist bombings of Pan Am Flight 103 and UTA Flight 772, pursuant to S.C. Resolutions 748 (1992) and 883 (1993); sanctions against Al Qaida and the Taliban under Resolution 1267 (1999) and subsequently against the Islamic State in Iraq and the Levant (ISIL)/Da'esh under Resolutions 1989 (2011) and 2253 (2015).
32 Bank Markazi Iran v. Peterson, 578 U.S. 1 (2016).
33 Certain Iranian Assets (Iran v. U.S.), Preliminary Objections, 2019 ICJ.

When the Court reaches the merits of Certain Iranian Assets, it may well be confronted with questions of first impression concerning the potential justification of alleged U.S. treaty violations as countermeasures against prior wrongful acts of Iran. Indeed, several commentators have suggested that the U.S. suspension of Iran's immunity from execution could not be justified under ARSIWA's countermeasures criteria, principally because of doubts about the reversibility of measures of execution against Iranian assets.[34] Although the issues as posed in the pending case involve only the bilateral treaty relationship between Iran and the United States, it would not be farfetched to envision other factual scenarios under which states making common cause against a state sponsor of terrorism might undertake collective countermeasures.

Many treaties of widespread multilateral participation prohibit terrorist activity and require all states parties to cooperate in suppressing terrorism, inter alia by ensuring that all terrorist suspects will either be prosecuted in the states where they are found or turned over to another state for purposes of prosecution. Many states and scholars consider that such treaties of the aut dedere aut judicare type support the exercise of universal jurisdiction, to allow criminal proceedings to proceed even in the absence of the usual links of territoriality or nationality of the actor or the victim. In the sense comprehended by "universal" jurisdiction, perhaps arguments grounded in the interests of "the international community as a whole" would likewise be sufficient to justify collective countermeasures against a state responsible for terrorist activity.

However, the continuing controversies over general definitions of terrorism, and the non-party status of some states implicated in support for terrorist activities, could undercut the viability of such arguments – at least under a narrow approach to ARSIWA's countermeasures criteria.

34 For references and quotations, see my contribution to the Berkeley symposium in memory of David Caron, published as Lori Fisler Damrosch, The Legitimacy of Economic Sanctions as Countermeasures for Wrongful Acts, 37 Berkeley J. Int'l L. 249, 261-262 (2019).

As with diplomatic law and nonproliferation regimes, collective countermeasures for antiterrorism purposes could readily involve cyber operations – either because the terrorist activities themselves took place in cyberspace, or because the responsive collective countermeasures might have a cyber component.

III. Conclusion

As the scenarios involving diplomatic relations, nonproliferation, and terrorism suggest, the availability of collective countermeasures can strengthen legal regimes involving interests transcending those of states directly injured by particular violations. Yet it is not necessarily clear under a rigid interpretation of ARSIWA's provisions – facilely imputing to ARSIWA the law-like qualities of black-letter rules, as if states had formally adopted them, which is not the case with the countermeasures rules – that obligations under the relevant treaties or their parallel bodies of customary international law would meet the relatively stringent standards of obligations owed to "the international community as a whole," or of peremptory norms that are hierarchically superior to other obligations, or that particular breaches would qualify as "serious" enough to entail a "gross or systematic failure" to fulfill such obligations. Insistence that only "injured states" are lawfully entitled to respond with countermeasures would leave a large enforcement gap in regimes that are underenforced under the best of circumstances. Prudently applied, collective countermeasures should strengthen enforcement capacity for the international legal system as a whole. Even so, the arguments for collective countermeasures need not stand or fall on whether greater economic leverage would predictably cause violating states to terminate unlawful behavior after embarking on a violation. Equally important, the knowledge that collective countermeasures are a lawful response to any unlawful act can strengthen collective normative commitments across the board and contribute to potential deterrence of future violations.

The Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector

List of Signatories

1. Nele Achten, Adviser at ICT4Peace foundation; affiliate at Harvard's Berkman Klein Center for Internet and Society
2. Mark D. Agrast, Executive Director, American Society of International Law
3. Dapo Akande, Professor of Public International Law, Co-Director, Oxford Institute for Ethics, Law & Armed Conflict (ELAC), University of Oxford
4. Katya Alkhateeb, Senior Research Officer, School of Law & Human Rights Centre, University of Essex
5. Daniel Álvarez-Valenzuela, Professor of Law, University of Chile School of Law, Academic Coordinator, Centre for Information Technology Law Studies (CEDI)
6. Diane Marie Amann, Emily & Ernest Woodruff Chair in International Law and Faculty Co-Director, Dean Rusk International Law Center, University of Georgia School of Law
7. Catherine Amirfar, Partner, Debevoise & Plimpton LLP, former Counselor on International Law, U.S. State Department (2014-2016)
8. Joshua Andresen, Deputy Head of School and Senior Lecturer in National Security and Foreign Relations Law, School of Law, University of Surrey
9. Mahnoush H. Arsanjani, Former Director, Codification Division, Office of Legal Affairs, United Nations
10. Oscar Noé Ávila, President of the ISOC Cybersecurity SIG
11. Aslı Bâli, Professor of Law, UCLA School of Law
12. Steven J. Barela, Senior Research Fellow, University of Geneva
13. Eyal Benvenisti, Whewell Professor of International Law, University of Cambridge, C C Ng Fellow, Jesus College, Director of the Lauterpacht Centre for International Law
14. Daniel Bodansky, Regents' Professor, Sandra Day O'Connor College of Law, Arizona State University
15. Kristen Boon, Professor of Law, Seton Hall Law School
16. Antonio Remiro Brotons, Emeritus Professor of Public International Law, Universidad Autónoma Madrid

17. Russell Buchan, Senior Lecturer in International Law, University of Sheffield
18. Nicolás Carrillo-Santarelli, Associate Professor of International Law, La Sabana University, Colombia
19. Koldo Casla, Lecturer, School of Law, University of Essex
20. Anthony E Cassimatis, Professor of Law, University of Queensland
21. Kalliopi Chainoglou, Assistant Professor of International Law and International institutions, Department of International and European Studies, University of Macedonia (Greece)
22. Benarji Chakka, Professor of International Law, VIT-AP University School of Law (VSL), VIT-AP University, India
23. Alejandro Chehtman, Professor of International Law at Di Tella University, Argentina
24. Lilian Chenwi, Professor of Law, University of the Witwatersrand School of Law
25. Roger S. Clark, Board of Governors Professor, Rutgers Law School
26. Sarah H. Cleveland, Louis Henkin Professor of Human and Constitutional Rights, Columbia University Law School, Former Vice Chair, UN Human Rights Committee
27. Antonio Coco, Lecturer in Public International Law, University of Essex and Visiting Fellow at ELAC, University of Oxford
28. Federica Cristani, Senior Researcher, Institute of International Relations, Prague
29. Rebecca Crootof, Assistant Professor of Law, University of Richmond School of Law
30. Federica D'Alessandra, Executive Director of the Oxford Programme on International Peace and Security, Blavatnik School of Government, University of Oxford
31. Jean D'Aspremont, Chair in Public International Law, University of Manchester; Professor of International Law, Sciences Po School of Law
32. Lori Fisler Damrosch, Hamilton Fish Professor of International Law and Diplomacy, Columbia University Law School
33. Tom Dannenbaum, Assistant Professor of International Law, The Fletcher School of Law & Diplomacy, Tufts
34. Erika De Wet, Professor of International Law and Head of the Institute of International Law and International Relations, Faculty of Law, University of Graz
35. François Delerue, Research Fellow in Cyberdefense and International Law at

the Institut de Recherche stratégique de l'École militaire (IRSEM) and Adjunct Lecturer at Sciences Po, Paris, France

36. Diane Desierto, Associate Professor of Human Rights Law and Global Affairs, Keough School of Global Affairs, University of Notre Dame
37. Talita Dias, Postdoctoral Research Fellow, ELAC, University of Oxford
38. Heather Harrison Dinniss, Senior Lecturer in International Law, Centre for International and Operational Law, Swedish Defence University
39. William S. Dodge, Martin Luther King, Jr. Professor of Law and John D. Ayer Chair in Business Law, University of California, Davis, School of Law
40. Pavan Duggal, Advocate, Supreme Court of India, Founder-cum-Chancellor, Cyberlaw University
41. Brian Egan, Partner, Steptoe & Johnson LLP, Washington DC, former Legal Adviser, US Department of State, 2016-17
42. Kristen Eichensehr, Assistant Professor of Law, UCLA Law School
43. Graça Enes, Professor of Law, Faculty of Law of the University of Porto
44. Itay Epshtain, Senior Humanitarian Law and Policy Consultant, Humanitarian Policy
45. Carlos Espósito, Professor of International Law, Catedrático de Derecho internacional público, Universidad Autónoma de Madrid
46. Martin Faix, Senior Lecturer in International Law, Palacký University Olomouc/ Charles University in Prague, Czech Republic
47. David P. Fidler, Adjunct Senior Fellow for Cybersecurity and Global Health, Council on Foreign Relations
48. Eric Fripp, Barrister, Lamb Building, Temple EC4Y, London, UK; Senior Visiting Fellow, Refugee Law Initiative, School of Advanced Study, University of London
49. Hans-Peter Gasser, Former Senior Legal Advisor, ICRC
50. Robin Geiss, Professor and Chair of International Law and Security, University of Glasgow; Director, Glasgow Centre for International Law and Security (GCILS); Director, United Nations Institute for Disarmament Research
51. Geoff Gilbert, Professor of International Human Rights & Humanitarian Law, School of Law and Human Rights Centre, University of Essex
52. Chiara Giorgetti, Professor of Law, Richmond Law School; Chair, Academic Council, Institute for Transnational Arbitration
53. Laurent Gisel, Senior Legal Adviser and Cyber Team Leader, Legal Division,

International Committee of the Red Cross

54. Richard Goldstone, former Prosecutor International Criminal Tribunal for the former Yugoslavia, former Judge Constitutional Court of South Africa
55. Guy S. Goodwin-Gill, Professor of Law, University of New South Wales (UNSW), Andrew & Renata Kaldor Centre for International Refugee Law, UNSW, Emeritus Fellow, All Souls College, Oxford
56. Claudio Grossman, Professor of Law, Dean Emeritus, American University Washington College of Law
57. Oleg Gushchyn, Professor, Military Law Department, Taras Shevchenko National University of Kyiv, Ukraine
58. Ondrej Hamuľák, Senior lecturer in EU law, Faculty of Law, Palacký University Olomouc, Czech Republic
59. Adil Haque, Professor of Law and Judge Jon O. Newman Scholar, Rutgers Law School
60. Jakub Harasta, Assistant Professor, Faculty of Law, Masaryk University, Czech Republic
61. Oona A. Hathaway, Gerard C. and Bernice Latrobe Smith Professor of International Law, Counselor to the Dean, and Director of the Center for Global Legal Challenges, Yale Law School
62. Mohamed S. Helal, Assistant Professor of Law Moritz College of Law, The Ohio State University; Member, African Union Commission on International Law
63. Kevin Jon Heller, Professor at Australian National University and Associate Professor of Public International Law at the University of Amsterdam
64. Stacey Henderson, Lecturer, Adelaide Law School, The University of Adelaide
65. Lawrence Hill-Cawthorne, Associate Professor in Public International Law, School of Law, University of Reading
66. Moshe Hirsch, Professor of International Law, Maria Von Hofmannsthal Chair in International Law, Faculty of Law & Department of International Relations, Hebrew University of Jerusalem
67. Tamás Hoffmann, Senior Research Fellow, Centre for Social Sciences Institute for Legal Studies; Associate Professor, Corvinus University of Budapest
68. Duncan B. Hollis, Laura H. Carnell Professor of Law, Temple University School of Law
69. Tawanda Hondora, Solicitor and Executive Director, World Federalist Movement

– Institute for Global Policy (WFM-IGP)

70. Zhixiong Huang, Professor of International Law & Vice Dean, Wuhan University School of Law, China
71. Karen Hulme, Professor and Head of the School of Law, University of Essex; Peace, Security and Conflict Specialist Group Chair, International Union for Conservation of Nature (IUCN)
72. Rebecca Ingber, Associate Professor of Law, Boston University School of Law (current); Professor of Law, Benjamin N. Cardozo School of Law (as of July 1)
73. Eric Talbot Jensen, Robert W. Barker Professor of Law, Brigham Young University
74. Valentin Jeutner, Associate Professor of Law, Faculty of Law, Lund University
75. Derek Jinks, A.W. Walker Centennial Chair in Law, University of Texas School of Law
76. Stian Øby Johansen, Associate professor at the Centre for European Law at the University of Oslo
77. Kate Jones, Faculty of Law, University of Oxford
78. Ershadul Karim, Senior Lecturer, Faculty of Law, University of Malaya
79. Kadri Kaska, Head of Law Branch, NATO Cooperative Cyber Defence Centre of Excellence
80. Ido Kilovaty, Assistant Professor of Law, University of Tulsa College of Law
81. Stefan Kirchner, Associate Professor of Arctic Law and Adjunct Professor (dosentti) of Fundamental and Human Rights, University of Lapland, Rovaniemi, Finland
82. Harold Hongju Koh, Sterling Professor of International Law, Yale Law School, Legal Adviser (2009-13) and Assistant Secretary for Democracy, Human Rights and Labor (1998-2001), US Department of State
83. Claus Kreß, Professor and Director, Institute of International Peace and Security Law, University of Cologne
84. Heike Krieger, Professor of International and Public Law, Freie Universität Berlin
85. Masahiro Kurosaki, Associate Professor of International Law and Director of the Study of Law, Security and Military Operations, National Defense Academy of Japan
86. Aigerim Kussaiynkyzy, Senior lecturer of International law, Suleiman Demirel University, Kaskelen, Kazakhstan
87. O-Gon Kwon, President, Assembly of States Parties, International Criminal

Court, former Judge and Vice President, International Criminal Tribunal for the former Yugoslavia (Seoul, Republic of Korea)

88. Patryk I. Labuda, Postdoctoral Scholar, Fletcher School of Law and Diplomacy; Non-Resident Fellow, International Peace Institute
89. Henning Lahmann, Digital Society Institute, ESMT Berlin, Germany
90. Kobi Leins, Senior Research Fellow in Digital Ethics, University of Melbourne
91. Anthony Lester QC, Blackstone Chambers, London
92. Brianne McGonigle Leyh, Associate Professor of Human Rights Law and Global Justice, Utrecht University
93. Eliav Lieblich, Senior Lecturer, Buchmann Faculty of Law, Tel Aviv University
94. Rain Liivoja, Associate Professor of Law, University of Queensland
95. Maria Pilar Llorens, Postdoctoral Research Fellow (CONICET), CIJS (CONICET-UNC) and Lecturer in Public International Law, Facultad de Derecho, Universidad Nacional de Córdoba, Argentina
96. Marco Longobardo, Lecturer in International Law, University of Westminster
97. Asaf Lubin, Affiliate, Berkman Klein Center for Internet and Society, Harvard University; Associate Professor, Indiana University Maurer School of Law (beginning Fall 2020)
98. Doreen Lustig, Senior Lecturer, Tel Aviv University Faculty of Law
99. Fabrizio Marrella, Full Professor of International Law, University "Ca' Foscari" Venice, Italy
100. Maurice Mendelson QC, Blackstone Chambers Barristers; Emeritus Professor of International Law in the University of London
101. Bonita Meyersfeld, Associate Professor of Law, University of the Witwatersrand, South Africa
102. Tomohiro Mikanagi, Ministry of Foreign Affairs, Japan
103. Marko Milanovic, Professor of Public International Law, University of Nottingham School of Law
104. Samuel Moyn, Henry R. Luce Professor of Jurisprudence, Yale University
105. Harriet Moynihan, Senior Research Fellow, International Law Programme, Chatham House (Royal Institute of International Affairs)
106. Sean D. Murphy, Manatt/Ahn Professor of International Law, George Washington University Law School
107. Daragh Murray, Senior Lecturer, University of Essex School of Law & Human

Rights Centre

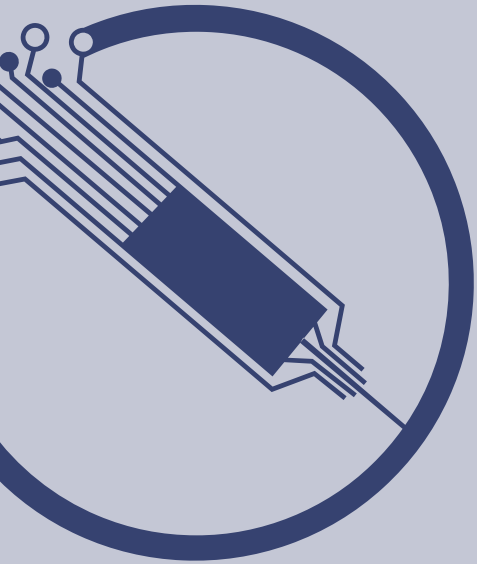
108. Andre Nollkaemper, Professor of Public International Law and Dean of the Amsterdam Law School at the University of Amsterdam
109. James C. O'Brien, Vice Chair, Albright Stonebridge Group
110. Phoebe Okowa, Professor of Public International Law, Queen Mary, University of London
111. Anne Peters, Director, Max Planck Institute for Comparative Public Law and International Law, Heidelberg, Germany
112. Alexandra Phelan, Assistant Professor at the Center for Global Health Science & Security, Georgetown University School of Medicine; Adjunct Professor of Law, Georgetown University Law Center, Washington, DC, United States
113. Mónica Pinto, Professor Emerita, Universidad de Buenos Aires, Facultad de Derecho, Argentina
114. Stephen Pomper, Senior Director for Policy, International Crisis Group; former U.S. State Department Assistant Legal Adviser for Political-Military Affairs
115. Michael Posner, Jerome Kohlberg Professor of Ethics and Finance, NYU Stern School of Business; Former Assistant Secretary of State for Democracy, Human Rights and Labor (2009-2013)
116. Anni Pues, Lecturer in International Law, Glasgow Centre for International Law and Security, University of Glasgow
117. Dainius Puras, UN Special rapporteur on the right to physical and mental health
118. Steven R. Ratner, Bruno Simma Collegiate Professor of Law, University of Michigan Law School
119. Paul S. Reichler, Partner, Chair of the International Litigation and Arbitration Department, Foley Hoag LLP, Washington, DC
120. Michael Reisman, Professor, Yale Law School
121. Przemysław Roguski, Lecturer in Law, Jagiellonian University in Kraków, Poland
122. Gabor Rona, Professor of Practice, Cardozo Law School
123. Hélène Ruiz-Fabri, Professor, Director of the Max Planck Institute Luxembourg for Procedural Law
124. Barrie Sander, Fellow, Fundação Getúlio Vargas, Brazil
125. Clara Sandoval, Professor, Co-Director – Essex Transitional Justice Network (ETJN), School of Law and Human Rights Centre, University of Essex
126. Andrew Sanger, University Lecturer in International Law, University of

Cambridge

127. Ben Saul, Challis Chair of International Law, Sydney Law School
128. Sergey Sayapin, Associate Professor of International and Criminal Law, School of Law, KIMEP University, Kazakhstan
129. Roman Schmidt-Radefeldt, Legal Advisor of international law, Research Services of the German Parliament (Deutscher Bundestag) and lecturer in international law, Humboldt-University Berlin
130. Michael N. Schmitt, Professor of International Law at the University of Reading and Francis Lieber Distinguished Scholar at the United States Military Academy (West Point)
131. John Shattuck, Professor of Practice in Diplomacy, Fletcher School of Law and Diplomacy, Tufts University; US Assistant Secretary of State for Democracy, Human Rights and Labor (1993-98); Ambassador to the Czech Republic (1998-2000); President Emeritus, Central European University
132. Bruno Simma, Judge at the Iran-United States Claims Tribunal; former Judge at the International Court of Justice; Professor of Law at the University of Michigan Law School, Ann Arbor, U.S.A (on leave)
133. Alfred H.A. Soons, Professor emeritus of public international law, Utrecht University School of Law, The Netherlands
134. Carsten Stahn, Professor of International Criminal Law and Global Justice, Leiden Law School and Queen's University Belfast
135. David P. Stewart, Professor from Practice, Georgetown University Law Center, Washington DC
136. Elizabeth Stubbins Bates, Junior Research Fellow in Law, Merton College, Oxford; Early Career Fellow, Bonavero Institute of Human Rights, University of Oxford; Research Fellow, ELAC
137. Csaba Törő, Associate Professor, Institute of Social Science and International Studies, Faculty of Law of the Károli Gáspár University of the Reformed Church in Hungary
138. Knut Traisbach, Adjunct Professor of Public International and Human Rights Law, University of Barcelona and University Ramon Llull, ESADE, Barcelona, Spain
139. Tuba Turan, Lecturer in Law, School of Law and Human Rights Centre, University of Essex
140. Tsvetelina van Benthem, Lecturer in International Law, Oxford Diplomatic

Studies Programme; Research Officer, ELAC, University of Oxford

141. Larissa van den Herik, Professor of Public International Law, Grotius Centre for International Legal Studies, Leiden University
142. Liis Vihul, Founder and CEO, Cyber Law International
143. John Paolo Roberto A. Villasor, Dean and Professor of Law, UNO-Recoletos School of Law, Philippines
144. Michael Waibel, Professor of International Law, University of Vienna, Austria
145. Marek Jan Wasinski, Associate Professor, University of Lodz, Poland
146. Philippa Webb, Professor of Public International Law, King's College London
147. Leah West, Lecturer, Norman Paterson School of International Affairs, Carleton University, Canada
148. Alex Whiting, Professor of Practice, Harvard Law School
149. Ralph Wilde, Associate Professor of International Law, University College London, University of London
150. Elizabeth Wilmshurst, Distinguished Fellow, International Law Programme, Chatham House (Royal Institute of International Affairs)



The Second Oxford Statement on the International Law Protections of the Healthcare Sector During Covid-19: Safeguarding Vaccine Research

List of Signatories

1. Mark D. Agrast, Executive Director, American Society of International Law
2. Dapo Akande, Professor of Public International Law, Co-Director, Oxford Institute for Ethics, Law & Armed Conflict (ELAC), University of Oxford
3. Mariana Salazar Albornoz, Member of the Inter-American Juridical Committee
4. Katya Alkhateeb, Senior Research Officer, School of Law & Human Rights Centre, University of Essex
5. Daniel Álvarez-Valenzuela, Professor of Law, University of Chile School of Law; Academic Coordinator Centre for Information Technology Law Studies (CEDI)
6. Catherine Amirfar, Partner, Debevoise & Plimpton LLP, former Counselor on International Law, U.S. State Department (2014-2016)
7. Mahnoush Arsanjani, Former Director, Codification Division, Office of Legal Affairs, United Nations
8. Pouria Askary, Assistant Professor of International Law, Allameh Tabataba'i University (ATU), Iran
9. Helmut Philipp Aust, Professor of Public and International Law, Freie Universität Berlin
10. Eyal Benvenisti, Whewell Professor of International Law, University of Cambridge, C C Ng Fellow, Jesus College, Director of the Lauterpacht Centre for International Law
11. Antonio Remiro Brotons, Emeritus Professor of International Law, Universidad Autónoma de Madrid
12. Russell Buchan, Senior Lecturer in International Law, University of Sheffield
13. Başak Çalı, Professor of International Law at the Hertie School, Berlin and its Director of the Centre for Fundamental Rights
14. Nicolás Carrillo-Santarelli, Associate researcher of International Law, University of Monterrey (UDEM)
15. Koldo Casla, Lecturer, School of Law, University of Essex
16. Anthony E. Cassimatis, Professor of Law, University of Queensland
17. Kalliopi Chainoglou, Assistant Professor of International Law and International

Institutions, University of Macedonia

18. Benarji Chakka, Professor of International Law, VIT-AP University School of Law (VSL), VIT-AP University, India
19. Alejandro Chehtman, Professor of International Law at Di Tella University, Argentina
20. Roger S. Clark, Board of Governors Professor, Rutgers Law School
21. Sarah H. Cleveland, Louis Henkin Professor of Human and Constitutional Rights, Columbia University Law School, Former Vice Chair, UN Human Rights Committee
22. Antonio Coco, Lecturer in Public International Law, University of Essex and Visiting Fellow at ELAC, University of Oxford
23. Federica Cristani, Senior Researcher, Institute of International Relations, Prague
24. Rebecca Crootof, Assistant Professor of Law, University of Richmond School of Law
25. Federica D'Alessandra, Executive Director of the Oxford Programme on International Peace and Security, Blavatnik School of Government, University of Oxford
26. Jean D'Aspremont, Chair in Public International Law, University of Manchester; Professor of International Law, Sciences Po School of Law
27. Lori Fisler Damrosch, Hamilton Fish Professor of International Law and Diplomacy, Columbia University Law School
28. Tom Dannenbaum, Assistant Professor of International Law, The Fletcher School of Law & Diplomacy, Tufts University
29. François Delerue, Research Fellow in Cyberdefense and International Law at the Institut de Recherche stratégique de l'École militaire (IRSEM) and Adjunct Lecturer at Sciences Po, Paris, France
30. Diane Desierto, Associate Professor of Human Rights Law and Global Affairs, Keough School of Global Affairs, University of Notre Dame
31. Talita Dias, Postdoctoral Research Fellow, ELAC, University of Oxford
32. William S. Dodge, Martin Luther King Jr Professor of Law, University of California, Davis, School of Law
33. Jessica Dorsey, Assistant Professor of International and European Law, Utrecht University School of Law, The Netherlands
34. Jeffrey L. Dunoff, Laura H. Carnell Professor of Law, Temple University Beasley

School of Law

35. Mark Eccleston-Turner, Senior Lecturer of Global Health Law, King's College London
36. Kristen E. Eichensehr, Martha Lubin Karsh and Bruce A. Karsh Bicentennial Professor of Law, University of Virginia School of Law
37. Benjamin Ferencz, sole surviving Nuremberg war crimes Prosecutor
38. Serena Forlati, Associate Professor, University of Ferrara, Italy
39. Chiara Giorgetti, Professor of Law, Richmond Law School
40. Guy S. Goodwin-Gill, Professor of Law, University of New South Wales (UNSW), Andrew & Renata Kaldor Centre for International Refugee Law, UNSW, Emeritus Fellow, All Souls College, Oxford
41. Claudio Grossman, Professor of Law, Dean Emeritus, American University Washington College of Law
42. Nienke Grossman, Professor of Law, Co-Director, Center for International and Comparative Law, University of Baltimore School of Law
43. Oleg Gushchyn, Professor, Military Law Department, Taras Shevchenko National University of Kyiv, Ukraine
44. Adil Haque, Professor of Law and Judge Jon O. Newman Scholar, Rutgers Law School
45. Jakub Harasta, Assistant Professor, Faculty of Law, Masaryk University, Czech Republic
46. Kevin Jon Heller, Professor of International Law and Security, University of Copenhagen, Professor of Law, Australian National University, Academic Member, Doughty Street Chambers
47. Stacey Henderson, Lecturer, Adelaide Law School
48. John Quentin Heywood, Associate Professor/Law Librarian, American University Washington College of Law, & Chair, AU Faculty Senate
49. Tamás Hoffmann, Senior Research Fellow, Centre for Social Sciences Institute for Legal Studies; Associate Professor, Corvinus University of Budapest
50. Duncan B. Hollis, Laura H. Carnell Professor of Law, Temple University School of Law; Member of the Inter-American Juridical Committee
51. Rebecca Ingber, Professor of Law, Benjamin N. Cardozo School of Law
52. Valentin Jeutner, Associate Professor of Law, Faculty of Law, Lund University
53. Derek Jinks, A.W. Walker Centennial Chair in Law, University of Texas School of

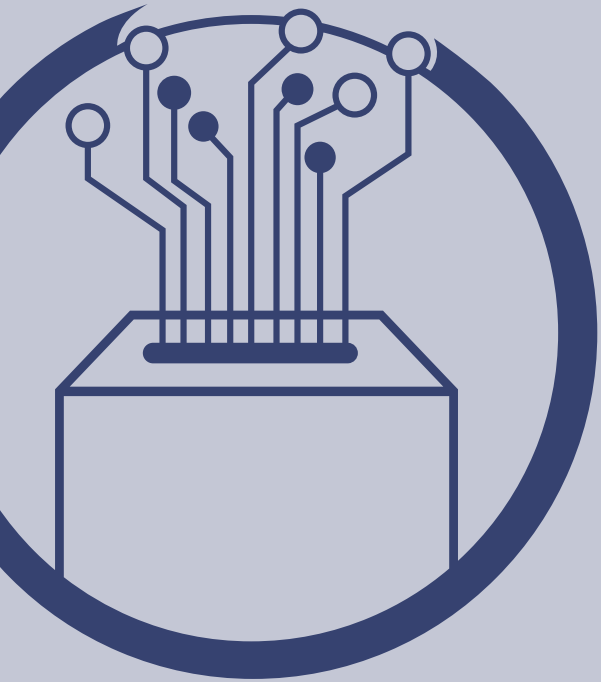
Law

54. Stian Øby Johansen, Associate professor at the Centre for European Law at the University of Oslo
55. Kate Jones, Faculty of Law, University of Oxford
56. Aonghus Kelly, Executive Director, Irish Rule of Law International
57. Jack Kenny, Research Assistant, ELAC
58. Shayan Ahmed Khan, Senior Research Associate, Research Society of International Law, Pakistan
59. Harold Hongju Koh, Sterling Professor of International Law, Yale Law School, Legal Adviser (2009-13) and Assistant Secretary for Democracy, Human Rights and Labor (1998-2001), US Department of State
60. Claus Kreß, Professor and Director, Institute of International Peace and Security Law, University of Cologne
61. Heike Krieger, Professor of International and Public Law, Freie Universität Berlin
62. Masahiro Kurosaki, Associate Professor of International Law and Director of the Study of Law, Security and Military Operations, National Defense Academy of Japan
63. O-Gon Kwon, President, Assembly of States Parties, International Criminal Court, former Judge and Vice President, International Criminal Tribunal for the former Yugoslavia (Seoul, Republic of Korea)
64. Henning Lahmann, Digital Society Institute, ESMT Berlin, Germany
65. Kobi Leins, Senior Research Fellow in Digital Ethics, Centre for AI and Digital Ethics, University of Melbourne; Non-Resident Fellow of the United Nations Institute for Disarmament Research
66. Eliav Lieblich, Senior Lecturer, Buchmann Faculty of Law, Tel Aviv University
67. Rain Liivoja, Associate Professor, University of Queensland Law School
68. Maria Pilar Llorens, Postdoctoral Research Fellow (CONICET), CIJS (CONICET-UNC) and Lecturer in Public International Law, Facultad de Derecho, Universidad Nacional de Córdoba, Argentina
69. Marco Longobardo, Lecturer in International Law, University of Westminster
70. Asaf Lubin, Associate Professor of Law, Indiana University Maurer School of Law; Faculty Associate, Berkman Klein Center for Internet and Society, Harvard University
71. Fabrizio Marrella, Full Professor of International Law, University "Ca' Foscari"

Venice, Italy; Professeur invité at the Sorbonne Law School, University Paris I Panthéon Sorbonne

72. Ralf Michaels, Director, Max Planck Institute for Comparative Law and Private International Law, Hamburg
73. Tomohiro Mikanagi, Ministry of Foreign Affairs, Japan
74. Marko Milanovic, Professor of Public International Law, University of Nottingham School of Law
75. José A. Moreno, Faculty Member, National University of Asunción, Paraguay; Member, Inter-American Juridical Committee
76. Samuel Moyn, Henry R. Luce Professor of Jurisprudence, Yale University
77. Natasa Nedeski, Assistant Professor Public International Law, University of Amsterdam
78. James C. O'Brien, Vice Chair, Albright Stonebridge Group
79. Mónica Pinto, Professor Emerita, Universidad de Buenos Aires, Facultad de Derecho
80. Erin Pobjie, Lecturer, University of Essex
81. Anni Pues, Lecturer in International Law, Glasgow Centre for International Law and Security, University of Glasgow
82. Paul S. Reichler, Partner, Chair of the International Litigation and Arbitration Department, Foley Hoag LLP, Washington, DC
83. Michael Reisman, Yale Law School
84. Alix Richard, Public International Lawyer, Port-au-Prince, Haiti; Member of the Inter-American Juridical Committee
85. Przemysław Roguski, Lecturer in Law, Jagiellonian University in Kraków, Poland
86. Gabor Rona, Professor of Practice and Director of the Law and Armed Conflict Project, Cardozo Law School
87. Hélène Ruiz-Fabri, Professor, Director of the Max Planck Institute Luxembourg for Procedural Law
88. Barrie Sander, Assistant Professor of International Justice, Leiden University
89. Andrew Sanger, University Lecturer in International Law, University of Cambridge
90. Roman Schmidt-Radefeldt, Legal Advisor of international law, Research Services of the German Parliament (Deutscher Bundestag) and lecturer in international law, Humboldt-University Berlin

91. Michael N. Schmitt, Professor of International Law at the University of Reading and Francis Lieber Distinguished Scholar at the United States Military Academy (West Point)
92. Afonso Seixas-Nunes, Assistant Professor, St Louis University
93. Shannon Raj Singh, Visiting Fellow of Practice, Oxford Program on International Peace and Security, ELAC
94. Ronald C. Slye, Professor of Law, Seattle University School of Law
95. Alfred H.A. Soons, Professor emeritus of public international law, Utrecht University School of Law, The Netherlands
96. David P. Stewart, Professor from Practice, Georgetown University Law Center, Washington DC
97. Elizabeth Stubbins Bates, Junior Research Fellow in Law, Merton College, Oxford; Early Career Fellow, Bonavero Institute of Human Rights, University of Oxford; Research Fellow, ELAC
98. Christian J. Tams, Chair of International Law, University of Glasgow; Director, Glasgow Centre of Int'l Law & Security
99. Ruti Teitel, Ernst C Stiefel Professor of Comparative Law, New York Law School
100. Csaba Törő, Associate Professor, Institute of Social Science and International Studies, Faculty of Law of the Károli Gáspár University of the Reformed Church in Hungary
101. Nicholas Tsagourias, Professor of International Law, University of Sheffield, Director of the Sheffield Centre for International and European Law
102. Tsvetelina van Benthem, Lecturer in International Law, Oxford Diplomatic Studies Programme; Research Officer, ELAC, University of Oxford
103. Liis Vihul, Founder and CEO, Cyber Law International
104. John Paolo Roberto A. Villasor, Dean and Professor of Law, UNO-Recoletos School of Law, Philippines
105. Michael Waibel, Professor of International Law, University of Vienna, Austria
106. Alex Whiting, Professor of Practice, Harvard Law School



The Oxford Statement on the International Law Protections Against Foreign Electoral Interference Through Digital Means

List of Signatories

1. Dapo Akande, Professor of Public International Law, Co-Director, Oxford Institute for Ethics, Law & Armed Conflict (ELAC), University of Oxford
2. Mariana Salazar Albornoz, Member of the Inter-American Juridical Committee, Professor of International Law, Universidad Iberoamericana
3. Kai Ambos, Professor and Chair of Criminal Law, Procedure, Comparative Law, International Criminal Law and Public International Law, Georg August Universität Göttingen, Germany
4. Joshua Andresen, Deputy Head of School and Senior Lecturer in National Security and Foreign Relations Law, School of Law, University of Surrey
5. Mahnoush H. Arsanjani, Former Director, Codification Division, Office of Legal Affairs, United Nations
6. Oscar Avila, Legal Counsel and President of the ISOC Cybersecurity SIG
7. Romel Regalado Bagares, Professorial Lecturer in International Law, Lyceum of the Philippines University College of Law
8. Karine Bannelier-Christakis, Associate Professor of International Law, Deputy Director of the Cyber Security Institute, University Grenoble Alpes
9. Steven J. Barela, Senior Research Fellow, Global Studies Institute and Member of the Law Faculty at the University of Geneva
10. Richard Barnes, Professor of International Law, School of Law, University of Lincoln
11. Pnina Sharvit Baruch, Senior Research Fellow and Head of Program on Law and National Security, Israel Institute for National Security Studies
12. Gary Bass, Professor of Politics and International Affairs, Princeton University
13. Eyal Benvenisti, Whewell Professor of International Law, University of Cambridge, C C Ng Fellow, Jesus College, Director of the Lauterpacht Centre for International Law
14. Susan H. Bitensky, Professor of Law, Michigan State University College of Law
15. Ziv Bohrer, Senior Lecturer in International Law, Faculty of Law, Bar-Ilan University

16. Christopher J. Borgen, Professor of Law and Co-Director, Center for International and Comparative Law, St. John's University School of Law
17. Michael Bothe, Professor emeritus of Public law, Law School, J.W. Goethe University, Frankfurt/Main
18. Tess Bridgeman, former Special Assistant to the President, Associate White House Counsel, and Deputy Legal Adviser to the National Security Council; Co-Editor-in-Chief, Just Security
19. Chester Brown, Professor of International Law and International Arbitration, The University of Sydney Law School
20. Russell Buchan, Senior Lecturer in International Law, University of Sheffield
21. Emiliano Buis, Professor of International Law, University of Buenos Aires
22. Michael Byers, Professor & Canada Research Chair in Global Politics and International Law, University of British Columbia
23. Nicolás Carrillo-Santarelli, Associate Researcher of the Institute of Human Rights and Business, UDEM University
24. Benarji Chakka, Professor of International Law, VIT-AP University School of Law (VSL), VIT-AP University, India
25. Théodore Christakis, Professor of International and European Law, Chair Legal and Regulatory Implications of Artificial Intelligence, University Grenoble Alpes
26. Roger S. Clark, Board of Governors Professor, Rutgers Law School
27. Antonio Coco, Lecturer in Public International Law, University of Essex and Visiting Fellow at ELAC, University of Oxford
28. Camilla Guldahl Cooper, Associate professor at the Norwegian Defence University College, Oslo
29. Geoffrey S. Corn, Gary A. Kuiper Distinguished Professor of National Security Law, South Texas College of Law Houston
30. Emily Crawford, Associate Professor, Sydney Law School, The University of Sydney
31. Federica Cristani, Senior Researcher, Institute of International Relations, Prague
32. Robert Cryer, Professor of International and Criminal Law, University of Birmingham, United Kingdom and Extraordinary Professor of Law, University of the Free State, South Africa
33. Federica D'Alessandra, Executive Director, Oxford Program on International Peace and Security, ELAC

34. Tom Dannenbaum, Assistant Professor of International Law, The Fletcher School of Law & Diplomacy, Tufts
35. Margaret M. deGuzman, James E. Beasley Professor of Law and Co-director of the Institute for International Law and Public Policy at Temple University Beasley School of Law
36. François Delerue, Research Fellow in Cyberdefense and International Law at the Institut de Recherche stratégique de l'École militaire (IRSEM) and Adjunct Lecturer at Sciences Po, Paris, France
37. Talita Dias, Postdoctoral Research Fellow, ELAC, University of Oxford
38. Jessica Dorsey, Assistant Professor of International and European Law, Utrecht University School of Law
39. Max du Plessis SC, Adjunct Professor, Nelson Mandela University and Senior Researcher, Institute for Security Studies
40. Pavan Duggal, Advocate, Supreme Court of India, Founder-cum-Chancellor, Cyberlaw University
41. Alonso Gurmendi Dunkelberg, Assistant Professor, Universidad del Pacífico, Peru
42. Jeffrey Dunoff, Laura H. Carnell Professor of Law, Temple University School of Law
43. Pierre-Marie Dupuy, Professor of Public International Law, Emeritus - Paris University (Panthéon-Assas), Graduate Institute of International and Development Studies -Geneva
44. Kristen E. Eichensehr, Martha Lubin Karsh and Bruce A. Karsh Bicentennial Professor of Law, University of Virginia School of Law
45. Cesáreo Gutiérrez Espada, Emeritus professor of International Law, Universidad de Murcia, Spain
46. Dorothy Estrada-Tanck, Associate Professor of Public International Law and Director of the Legal Clinic, University of Murcia, Spain
47. Tom Farer, University Professor and Dean Emeritus (1996-2010), Josef Korbel School of International Studies, University of Denver
48. Benjamin B. Ferencz, former Nuremberg war crimes Prosecutor
49. David P. Fidler, Adjunction Senior Fellow for Cybersecurity and Global Health, Council on Foreign Relations
50. Dieter Fleck, Honorary President, International Society for Military Law and the Law of War

51. Micaela Frulli, Professor, Law Department, University of Florence
52. Alexandre Skander Galand, Postdoctoral Fellow, Centre for Fundamental Rights, Hertie School, Berlin's University of Governance
53. Hans-Peter Gasser, former senior legal advisor, International Committee of the Red Cross (ICRC), Geneva
54. Robin Geiss, Professor and Chair of International Law and Security, University of Glasgow; Director, Glasgow Centre for International Law and Security (GCILS); Director, United Nations Institute for Disarmament Research
55. Geoff Gilbert, Professor of International Human Rights & Humanitarian Law, School of Law and Human Rights Centre, University of Essex
56. Chiara Giorgetti, Professor of Law, Richmond Law School
57. Guy S. Goodwin-Gill, Professor of Law, University of New South Wales (UNSW), Andrew & Renata Kaldor Centre for International Refugee Law, UNSW; Emeritus Fellow, All Souls College, Oxford
58. Gregory S. Gordon, Professor of Law, The Chinese University of Hong Kong
59. Charalee Graydon, Professor of Mediation and Conflict Resolution, EUCLID University, Member of Climate Change Policy Project, Mediators Beyond Borders International, Climate Change Policy Project
60. James A. Green, Professor of Public International Law, School of Law University of Reading
61. Oren Gross, Irving Younger Professor of Law, University of Minnesota Law School
62. Nienke Grossman, Professor of Law; Co-Director, Center for International and Comparative Law, University of Baltimore School of Law
63. Patrycja Grzebyk, Professor of Law, University of Warsaw
64. Douglas Guilfoyle, Associate Professor of International and Security Law, University of New South Wales Canberra
65. Oleg Gushchyn, Professor, Military Law Department, Taras Shevchenko National University of Kyiv, Ukraine
66. Steven Haines, Professor of Public International Law, University of Greenwich
67. Monica Hakimi, James V. Campbell Professor of Law, University of Michigan Law School
68. Françoise J. Hampson, Professor Emeritus, Law School & Human Rights Centre, University of Essex
69. Adil Haque, Professor of Law and Judge Jon O. Newman Scholar, Rutgers Law

School

70. Jakub Harasta, Assistant Professor, Faculty of Law, Masaryk University, Czech Republic
71. Kevin Jon Heller, Professor of International Law and Security, University of Copenhagen (Centre for Military Studies); Professor of Law, Australian National University
72. Christian Henderson, Professor of International Law, University of Sussex
73. Stacey Henderson, Lecturer of Law, Adelaide Law School, The University of Adelaide
74. John Quentin Heywood, Associate Professor, American University Washington College of Law
75. Tamás Hoffmann, Senior Research Fellow, Centre for Social Sciences Institute for Legal Studies; Associate Professor, Corvinus University of Budapest
76. Duncan B. Hollis, Laura H. Carnell Professor of Law, Temple University School of Law
77. María-José Cervell Hortal, tenured professor of Public International Law, Universidad de Murcia, Spain
78. Kristine Huskey, Clinical Professor of Law, University of Arizona James E. Rogers College of Law
79. Alfonso J. Iglesias Velasco, Professor of International Law, Autonomous University of Madrid
80. Mark Janis, formerly Fellow of Exeter College & Reader in Law, University of Oxford
81. Eric Talbot Jensen, Robert W. Barker Professor of Law, Brigham Young University
82. Derek Jinks, A.W. Walker Centennial Chair in Law, University of Texas School of Law
83. Kate Jones, Faculty of Law, University of Oxford
84. Kadri Kaska, Head of Law Branch, NATO Cooperative Cyber Defence Centre of Excellence
85. David Kaye, Professor of Law, UC Irvine School of Law, UN Special Rapporteur (2014-2020)
86. Shayan Ahmed Khan, Senior Research Associate, Research Society of International Law
87. Ido Kilovaty, Assistant Professor of Law, University of Tulsa College of Law

88. Jan Klabbers, Professor of International Law, University of Helsinki
89. Pierre Klein, Professor, Centre of International Law, Université libre de Bruxelles, Belgium
90. Bernhard Koch, Deputy Director Institute of Theology and Peace Hamburg; Co-Teacher Ethics at the ICMM Centre of Reference for Education on IHL and Ethics Zurich
91. Harold Hongju Koh, Sterling Professor of International Law, Yale Law School, Legal Adviser (2009-13) and Assistant Secretary for Democracy, Human Rights and Labor (1998-2001), US Department of State
92. Robert Kolb, Professor in Public International Law, University of Geneva
93. David Kretzmer, Emeritus Professor of international Law, Hebrew University of Jerusalem
94. Leonhard Kreuzer, Research Fellow, Max Planck Institute for Comparative Public Law and International Law, Heidelberg, Germany
95. Masahiro Kurosaki, Associate Professor of International Law and Director of the Study of Law, Security and Military Operations, National Defense Academy of Japan
96. Patryk I. Labuda, Postdoctoral Fellow, Amsterdam Center for International Law
97. Henning Lahmann, Senior Researcher, Digital Society Institute, ESMT Berlin
98. Kobi Leins, Senior Research Fellow in Digital Ethics, Centre for AI and Digital Ethics; Non-Resident Fellow, United Nations Institute for Disarmament
99. Gabriel M. Lentner, Assistant Professor of International Law and Arbitration, Danube University Krems, Austria
100. Rain Liivoja, Associate Professor of Law, University of Queensland
101. Maria Pilar Llorens, Postdoctoral Research Fellow (CONICET), CIJS (CONICET-UNC) and Lecturer in Public International Law, Facultad de Derecho, Universidad Nacional de Córdoba, Argentina
102. Marco Longobardo, Lecturer in International Law, University of Westminster
103. Juan Jorge Piernas López, Tenured Professor of Public International Law, University of Murcia, Spain
104. Asaf Lubin, Associate Professor of Law, Indiana University Maurer School of Law; Faculty Associate, Berkman Klein Center for Internet and Society, Harvard University
105. Fabrizio Marrella, Full Professor of International Law and Pro-Vice-Chancellor for

International Relations, "Ca' Foscari" University of Venice, Italy; Professeur invité at the Sorbonne Law School, University Paris I Panthéon Sorbonne

106. Maurice Mendelson QC, Blackstone Chambers Barristers; Emeritus Professor of International Law in the University of London
107. Errol P. Mendes, Professor, University of Ottawa; President, International Commission of Jurists, Canadian Section
108. Tomohiro Mikanagi, Ministry of Foreign Affairs, Japan
109. Marko Milanovic, Professor of Public International Law, University of Nottingham School of Law
110. Alex Mills, Professor of Public and Private International Law, Faculty of Laws, UCL
111. Tal Mimran, Lecturer of Public International Law and Research Fellow, Hebrew University of Jerusalem
112. Evgeni Moyakine, Assistant Professor of IT law, University of Groningen
113. Harriet Moynihan, Senior Research Fellow, International Law Programme, Chatham House (Royal Institute of International Affairs)
114. Sean D. Murphy, Manatt/Ahn Professor of International Law, George Washington University Law School
115. Roda Mushkat, Professor of International Law, School of Advanced International Studies (SAIS), Johns Hopkins University
116. Valère Ndior, Professor of International Law, Bretagne occidentale University, France
117. Michael A. Newton, Professor of the Practice of Law, Vanderbilt University Law School
118. James C. O'Brien, Vice Chair, Albright Stonebridge Group
119. Roger O'Keefe, Professor of International Law, Bocconi University and Honorary Professor of Law, University College London
120. Stefan Oeter, Professor of, Public International Law, University of Hamburg
121. Jens David Ohlin, Vice Dean and Professor of Law, Cornell Law School
122. Obiora Chinedu Okafor, Professor and York Research Chair in International and Transnational Legal Studies, Osgoode Hall Law School, York University, Toronto, Canada
123. Sejal Parmar, School of Law, University of Sheffield
124. Andreas Paulus, Professor, University of Goettingen, Germany

125. Jordan J. Paust, Professor Emeritus, University of Houston Law Center
126. Mónica Pinto, Professor Emerita, Universidad de Buenos Aires, Facultad de Derecho, Argentina
127. Erin Pobjie, Senior Research Fellow, Max Planck Institute for Comparative Public Law and International Law, Heidelberg, Germany
128. Anni Pues, Lecturer in International Law, Glasgow Centre for International Law and Security, University of Glasgow
129. Steven R. Ratner, Bruno Simma Collegiate Professor of Law, Director, University of Michigan Donia Human Rights Center, University of Michigan Law School
130. Michael Reisman, Professor Yale Law School
131. Henry J. Richardson III, Professor of Law, Temple University School of Law
132. José Antonio Moreno Rodríguez, Member of the Inter-American Juridical Committee
133. Przemysław Roguski, Lecturer in Law, Jagiellonian University in Kraków, Poland
134. Marco Roscini, Professor of International Law, Westminster Law School, University of Westminster
135. Eric P. Rudge, Judge First and Third Cantonal Court of Suriname, Acting Member of the High Court of Justice in Suriname, Member of the Inter-American Juridical Committee of the O.A.S.
136. Hélène Ruiz Fabri, Professor of international law, Max Planck Institute Luxembourg for Procedural law and Sorbonne Law School
137. Leila Nadya Sadat, President, International Law Association (American Branch); Special Adviser on Crimes Against Humanity, International Criminal Court Prosecutor; James Carr Professor of International Criminal Law, Director, Whitney R. Harris World Law Institute, Washington University School of Law
138. Barrie Sander, Assistant Professor of International Justice, Leiden University - Faculty of Governance and Global Affairs
139. Andrew Sanger, University Lecturer in International Law, University of Cambridge, and Fellow of Corpus Christi College and of the Lauterpacht Centre for International Law
140. Arman Sarvarian, Senior Lecturer in Public International Law, University of Surrey
141. Marco Sassòli, Professor of International Law, University of Geneva, Switzerland
142. Ben Saul, Challis Chair of International Law, Sydney Law School

143. Sergey Sayapin, Associate Professor and Associate Dean, School of Law, KIMEP University
144. David J. Scheffer, Clinical Professor Emeritus, Northwestern University Pritzker School of Law
145. Roman Schmidt-Radefeldt, Legal Advisor of international law, Research Services of the German Parliament (Deutscher Bundestag) and lecturer in International Law, Humboldt-University Berlin
146. Michael N. Schmitt, Professor of International Law at the University of Reading and Francis Lieber Distinguished Scholar at the United States Military Academy (West Point)
147. Iain G. M. Scobbie, Professor of Public International Law, Director of the Manchester International Law Centre, University of Manchester
148. Irene Vázquez Serrano, Assistant Professor of International Law, University of Murcia, Spain
149. Bruno Simma, Member, Iran-United States Claims Tribunal, former Judge at the International Court of Justice, Professor of Law, University of Michigan Law School, Ann Arbor, U.S.A.
150. Robert D. Sloane, Professor of Law and R. Gordon Butler Scholar in International Law, Boston University School of Law
151. David Sloss, John A. and Elizabeth H. Sutro Professor of Law, Santa Clara University School of Law
152. Ronald C. Slye, Professor of Law, Seattle University School of Law
153. Peter J. Spiro, Charles R. Weiner Professor of Law, Co-Director, Institute for International Law and Public Policy, Temple University School of Law
154. Ralph G. Steinhardt, Lobingier Professor of Comparative Law & Jurisprudence; Co-Founder, GW-Oxford Programme in International Human Rights Law, The George Washington University Law School
155. Dale Stephens, Professor of Law, The University of Adelaide Law School
156. Surya P. Subedi, QC, OBE, DCL, Professor, School of Law, University of Leeds, England; Barrister, Three Stone Chambers, Lincoln's Inn, London
157. James Summers, Senior Lecturer and Director of the Centre for International Law and Human Rights, Law School, Lancaster University
158. Shana Tabak, Executive Director, Tahirih Justice Center
159. Stefan Talmon, Professor and Director, Institute for Public International Law

University of Bonn, and Visiting Fellow, All Souls College, Oxford

160. Ruti Teitel, Ernst C Stiefel Professor of Comparative Law, Director, Institute on Global Law, Justice and Policy, New York Law School
161. Patrick Terry, Dean, Faculty of Law, University of Public Administration Kehl, Germany
162. Nicholas Tsagourias, Professor of International Law, University of Sheffield
163. Tsvetelina van Benthem, Lecturer in International Law, Oxford Diplomatic Studies Programme; Research Officer, ELAC, University of Oxford
164. Willem van Genugten, em. Professor of International Law, Tilburg University
165. Liis Vihul, Founder and CEO, Cyber Law International
166. John Paolo Roberto A. Villasor, Dean and Professor of Law, UNO-Recoletos School of Law, Philippines
167. Wolff Heintschel von Heinegg, Professor of Public International Law and European Law, European University, Frankfurt (Oder)
168. Michael Waibel, Professor of International Law, University of Vienna, Austria
169. Christopher Waters, Dean, Faculty of Law, University of Windsor, Canada
170. Eliza Watt, Lecturer in Law and Researcher in Mass Cyber Surveillance and International Human Rights, Middlesex University, London
171. Steven Wheatley, Professor of International Law, University of Lancaster
172. Ralph Wilde, Associate Professor of International Law, University College London, University of London
173. Pål Wrange, Professor of International Law, Director, Stockholm Centre for International Law and Justice, Stockholm University

The Oxford Statement on the International Law Protections in Cyberspace: The Regulation of Information Operations and Activities

List of Signatories

1. Dapo Akande, Professor of Public International Law, Co-Director, Oxford Institute for Ethics, Law & Armed Conflict (ELAC), University of Oxford
2. Mariana Salazar Albornoz, Rapporteur on International Law Applicable to Cyberspace, InterAmerican Juridical Committee
3. Daniel Álvarez-Valenzuela, Professor of Law, University of Chile School of Law, Academic Coordinator, Centre for Information Technology Law Studies (CEDI)
4. Kai Ambos, Professor and Chair of Criminal Law, Procedure, Comparative Law, International Criminal Law and Public International Law, Georg August Universität Göttingen, Germany
5. Pouria Askary, Associate Professor of International Law, Faculty of Law and Political Science, Allameh Tabataba'i University (ATU), Iran
6. Romel Regalado Bagares, Professorial Lecturer, Lyceum of the Philippines University College of Law, San Sebastian College Recoletos Manila, Graduate School of Law
7. William Banks, Board of Advisers Distinguished Professor emeritus, Syracuse University College of Law, Maxwell School of Citizenship & Public Affairs
8. Steven J. Barela, Senior Research Fellow, University of Geneva
9. Nehal Bhuta, Chair of Public International Law, University of Edinburgh
10. Ziv Bohrer, Senior Lecturer, Bar-Ilan University Faculty of Law
11. William Henry Boothby, Honorary Professor, Australian National University, Canberra
12. Michael Bothe, Professor emeritus of Public Law, School of Law, J.W. Goethe University Frankfurt/Main
13. Chester Brown, Professor of International Law and International Arbitration, University of Sydney
14. Marcel Brus, Professor of Public International Law, University of Groningen, The Netherlands
15. Russell Buchan, Senior Lecturer in International Law, University of Sheffield
16. Anne-Marie Buzatu, Vice President and Chief Operations Officer, ICT4Peace

Foundation

17. Michael Byers, Professor & Canada Research Chair in Global Politics and International Law, University of British Columbia
18. Nicolás Carrillo-Santarelli, Associate Researcher, Institute of Human Rights and Business, University of Monterrey (UDEM), and Professor of the Master's Programme in International Law, La Sabana University
19. Benarji Chakka, Professor of International Law, VIT-AP University School of Law, India
20. Alejandro Chehtman, Professor of Law, Universidad Torcuato Di Tella, Argentina
21. Roger S. Clark, Board of Governors Professor, Rutgers Law School
22. Antonio Coco, Lecturer in Public International Law, University of Essex and Visiting Fellow at ELAC, University of Oxford
23. Rebecca Crootof, Assistant Professor of Law, University of Richmond School of Law
24. Federica D'Alessandra, Executive Director, Oxford Program on International Peace and Security, ELAC
25. Tom Dannenbaum, Assistant Professor of International Law, The Fletcher School of Law & Diplomacy, Tufts
26. Margaret M. deGuzman, James E. Beasley Professor of Law, Temple University Beasley School of Law
27. François Delerue, Research Fellow in Cyberdefense and International Law at IRSEM & Lecturer at Sciences Po
28. Diane Desierto, Professor of Law and Global Affairs, LLM Faculty Director, Notre Dame Law School and Keough School of Global Affairs
29. Talita Dias, Shaw Foundation Junior Research Fellow, Jesus College, Oxford; Postdoctoral Research Fellow, ELAC, University of Oxford
30. Jessica Dorsey, Assistant Professor of International and European Law, Utrecht University School of Law, The Netherlands; Associate Fellow, International Center for Counterterrorism-The Hague
31. Dr. Pavan Duggal, Advocate, Supreme Court of India, Founder-cum-Chancellor, Cyberlaw University and Chairman, International Commission on Cyber Security Law
32. Jeffrey L. Dunoff, Laura H. Carnell Professor of Law, Temple University Beasley School of Law

33. Kristen Eichensehr, Martha Lubin Karsh and Bruce A. Karsh Bicentennial Professor of Law, University of Virginia School of Law
34. Martin Faix, Senior Lecturer in International Law, Palacký University Olomouc/ Charles University in Prague
35. Tom Farer, University Professor and Dean Emeritus (1996-2010), Josef Korbel School of International Studies, University of Denver
36. Benjamin Ferencz, Chief Prosecutor, United States of America v. Otto Ohlendorf et al., Case IX of the Subsequent Proceedings at Nuremberg 1947-1948, (the "Einsatzgruppen" Case)
37. David P. Fidler, Senior Fellow for Cybersecurity and Global Health, Council on Foreign Relations
38. Malgosia Fitzmaurice, Professor of International Law, Queen Mary University of London
39. Micaela Frulli, Professor, Law Department, University of Florence
40. Gloria Gaggioli, Associate Professor of Public International Law, University of Geneva and Director of the Geneva Academy of International Humanitarian Law and Human Rights
41. Chiara Giorgetti, Professor of Law, Richmond Law School
42. Richard J. Goldstone, Retired Justice of the Constitutional Court of South Africa, former Chief Prosecutor of the ICTY and ICTR
43. Guy S. Goodwin-Gill, Professor of Law, University of New South Wales (UNSW), Andrew & Renata Kaldor Centre for International Refugee Law, UNSW; Emeritus Fellow, All Souls College, Oxford
44. James A. Green, Professor of Public International Law, School of Law, University of Reading
45. Patrycja Grzebyk, Associate Professor, University of Warsaw
46. Douglas Guilfoyle, Associate Professor of International and Security Law, University of New South Wales Canberra
47. Oleg Gushchyn, Professor, Military Law Department, Taras Shevchenko National University of Kyiv, Ukraine
48. Samuli Haataja, Senior Lecturer, Griffith University, Australia
49. Michael Hamilton, Associate Professor of Public Protest Law, University of East Anglia
50. Jakub Harasta, Assistant Professor, Faculty of Law, Masaryk University, Czech

Republic

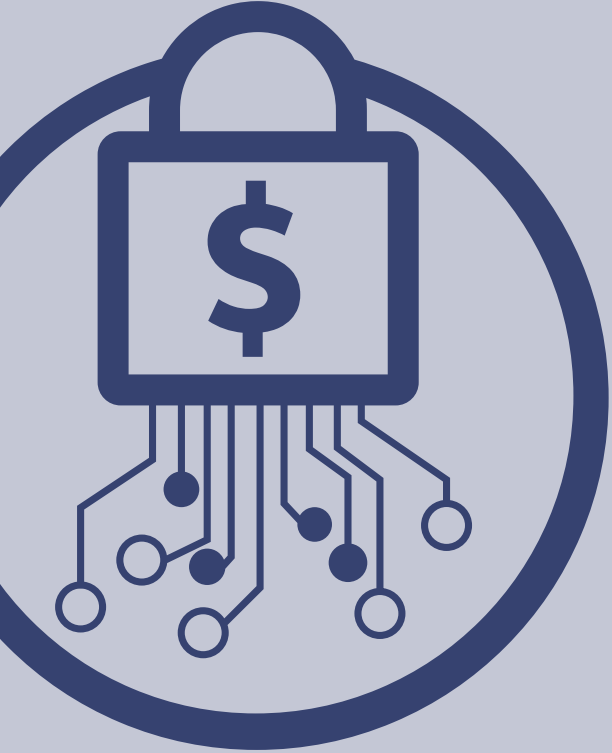
51. Kevin Jon Heller, Professor of International Law and Security, University of Copenhagen (Centre for Military Studies); Professor of Law, Australian National University
52. Christian Henderson, Professor of International Law, University of Sussex
53. Tamás Hoffmann, Senior Research Fellow, Centre for Social Sciences Institute for Legal Studies; Associate Professor, Corvinus University of Budapest
54. Duncan B. Hollis, Laura H. Carnell Professor of Law, Temple University School of Law
55. María José Cervell Hortal, Professor of Public International Law, University of Murcia, Spain
56. Deborah Housen-Couriel, The Federmann Cyber Security Research Center at the Hebrew University of Jerusalem; Chief Legal Officer and VP Regulation at Konfidas Digital Ltd.
57. Mark Weston Janis, William F Starr Professor of Law, University of Connecticut; formerly Reader in Law & Fellow of Exeter College, University of Oxford
58. Derek Jinks, A.W. Walker Centennial Chair, University of Texas School of Law
59. Kate Jones, Associate Fellow, Chatham House
60. Chimène Keitner, Alfred & Hanna Fromm Professor of International Law, UC Hastings School of Law, San Francisco
61. Ido Kilovaty, Associate Professor of Law, University of Tulsa College of Law
62. Robert Kolb, Professor in Public International Law, University of Geneva
63. Tetyana Krupiy, postdoctoral fellow, Tilburg University
64. Joanna Kulesza, tenured Professor of International Law and Internet Governance, University of Lodz, Poland
65. Masahiro Kurosaki, Associate Professor of International Law and Director of the Study of Law, Security and Military Operations, National Defense Academy of Japan
66. Henning Lahmann, Senior Researcher, Digital Society Institute, ESMT Berlin
67. Kobi Leins, Senior Research Fellow in Digital Ethics, University of Melbourne
68. Eliav Lieblich, Associate Professor, Buchmann Faculty of Law, Tel Aviv University
69. Maria Pilar Llorens, Postdoctoral Research Fellow (CONICET), CIJS (CONICET-UNC) and Lecturer in Public International Law, Facultad de Derecho, Universidad Nacional de Córdoba, Argentina

70. Marco Longobardo, Lecturer in International Law, University of Westminster
71. Asaf Lubin, Associate Professor of Law, Indiana University Maurer School of Law; Faculty Associate, Berkman Klein Center for Internet and Society, Harvard Law School; Affiliated Fellow, Information Society Project, Yale Law School
72. Fabrizio Marrella, Full Professor of International Law and Vice Rector for International Relations, "Ca' Foscari" University of Venice, Italy; Professeur invité at the Sorbonne Law School, University Paris I Panthéon Sorbonne
73. Errol P. Mendes, Professor, University of Ottawa; President, International Commission of Jurists, Canadian Section
74. Tomohiro Mikanagi, Ministry of Foreign Affairs, Japan
75. Marko Milanovic, Professor of Public International Law, University of Nottingham School of Law
76. Tal Mimran, Research Director of the Federmann Cyber Security Research Center (Law Program), Lecturer in Public International Law, Hebrew University of Jerusalem
77. Evgeni Moyakine, Assistant Professor in Law, University of Groningen
78. Samuel Moyn, Henry R. Luce Professor of Jurisprudence, Yale University
79. Harriet Moynihan, Senior Research Fellow, International Law Programme, Chatham House
80. Valère Ndior, Professor of International Law, Bretagne occidentale University, France
81. Michael Newton, Professor of the Practice of Law, Vanderbilt University Law School
82. James C. O'Brien, Vice Chair, Albright Stonebridge Group
83. Mary Ellen O'Connell, Robert and Marion Short Professor of Law and Research Professor of International Dispute Resolution, Kroc Institute for International Peace Studies, University of Notre Dame
84. Roger O'Keefe, Professor of International Law, Bocconi University
85. Stefan Oeter, Professor of Public Law and International Law, Faculty of Law, University of Hamburg
86. Obiora Okafor, Professor and York Research Chair in International and Transnational Legal Studies, Osgoode Hall Law School of York University, Toronto, Canada
87. Natalie Oman, Visiting Professor, Peter A. Allard School of Law, University of

British Columbia, Associate Professor, Legal Studies Program, University of Ontario Institute of Technology

88. Inger Österdahl, Professor of public international law, Uppsala University
89. Sejal Parmar, Lecturer, School of Law, University of Sheffield
90. Anni Pues, Lecturer in International Law, Glasgow Centre for International Law and Security, University of Glasgow
91. Qerim Qerimi, Professor of Public International Law, International Law of Human Rights and International Organizations, University of Prishtina & Visiting Professor, Law and Development Research Group – Faculty of Law, University of Antwerp; Member, Venice Commission of the Council of Europe
92. Przemysław Roguski, Lecturer in Law, Jagiellonian University in Kraków, Poland
93. Hélène Ruiz Fabri, Professor of International Law, Director of the Max Planck Institute Luxembourg for Procedural Law
94. Gianpaolo Maria Ruotolo, Full professor of international law, School of Law, University of Foggia
95. Leila Nadya Sadat, Special Adviser on Crimes Against Humanity, International Criminal Court Prosecutor, James Carr Professor of International Criminal Law, Washington University School of Law
96. Barrie Sander, Assistant Professor, Leiden University - Faculty of Governance and Global Affairs
97. Goran Sandić, MA, Belgrade Centre for Human Rights
98. Andrew Sanger, University Lecturer in International Law, University of Cambridge
99. Sergey Sayapin, Associate Professor and Associate Dean, School of Law, KIMEP University (Almaty, Kazakhstan)
100. Michael N. Schmitt, Professor of International Law at the University of Reading and G. Norman Lieber Distinguished Scholar at the United States Military Academy (West Point)
101. Irene Vázquez Serrano, Assistant professor of International Law, University of Murcia, Spain
102. Bruno Simma, Judge, Iran-United States Claims Tribunal, former Judge at International Court of Justice, Professor at the University of Michigan Law School, Ann Arbor, U.S.A., Professor (ret.) at Faculty of Law, University of Munich. Germany

103. David Sloss, John A. and Elizabeth H. Sutro Professor of Law, Santa Clara University
104. Ronald C. Slye, Professor of Law, Seattle University School of Law
105. Alfred H. A. Soons, Professor emeritus of public international law, Utrecht University School of Law, The Netherlands
106. Dale Stephens, Professor of Law, The University of Adelaide Law School
107. Surya P. Subedi QC, Professor of International Law, University of Leeds, UK
108. James Summers, Senior Lecturer in International Law; Director of the Centre for International Law and Human Rights, Lancaster University Law School
109. Patrick C. R. Terry, Dean & Professor of Law, University of Public Administration Kehl, Germany
110. Kimberley N. Trapp, Professor of Public International Law, University College London Faculty of Laws
111. Tsvetelina van Benthem, Lecturer in International Law, Oxford Diplomatic Studies Programme; Research Officer, ELAC, University of Oxford
112. Willem van Genugten, em. Professor of International Law, Tilburg University
113. Liis Vihul, Founder and CEO, Cyber Law International
114. Michael Waibel, Professor of International Law, University of Vienna, Austria
115. Christopher Waters, Professor, Faculty of Law, University of Windsor
116. Philippa Webb, Professor of Public International Law, King's College London
117. Leah West, Assistant Professor & Associate Director (Admissions and Recruitment), Norman Paterson School of International Affairs, Carleton University
118. Steven Wheatley, Professor of International Law, University of Lancaster
119. Ralph Wilde, Faculty of Laws, University College London
120. Pål Wrange, Professor of Public International Law & Director, Stockholm Center for International Law and Justice, Stockholm University
121. Binxin Zhang, Scholar in Political Science, Centre for International Studies, Sciences Po; Research Fellow, Centre for International Research and Policy



The Oxford Statement on the International Law Protections in Cyberspace: The Regulation of Ransomware Operations

List of Signatories

1. Dapo Akande, Professor of Public International Law, Co-Director, Oxford Institute for Ethics, Law & Armed Conflict (ELAC), University of Oxford
2. Mariana Salazar Albornoz, Member, Inter-American Juridical Committee (OAS) and Professor of International Law, Universidad Iberoamericana, Mexico City
3. Kai Ambos, Professor and Chair of Criminal Law, Procedure, Comparative Law, International Criminal Law and Public International Law, Georg August Universität Göttingen, Germany
4. Joshua Andresen, Deputy Head of School and Reader in National Security and Foreign Relations Law, School of Law, University of Surrey
5. Pouria Askary, Associate Professor of International Law, Allameh Tabataba'i University
6. William Banks, Board of Advisers Distinguished Professor, Syracuse University College of Law
7. Richard Barnes, Professor, The University of Lincoln
8. Orna Ben-Naftali, Professor of Law and Emile Zola Chair for Human Rights, The Striks Law Faculty, The College of Management Academic Studies, Israel
9. Nehal Bhuta, Chair of Public International Law, University of Edinburgh
10. Ziv Bohrer, Senior Lecturer in International Law, Faculty of Law, Bar-Ilan University
11. Michael Bothe, Professor emeritus of Public Law, J.W. Goethe University, Frankfurt/Main
12. Tomer Broude, Professor, Bessie & Michael Greenblatt, Q.C., Chair in Public and International Law, Faculty of Law and Department of International Relations, Hebrew University of Jerusalem
13. Chester Brown, Professor of International Law and International Arbitration, Sydney Law School, University of Sydney
14. Russell Buchan, Senior Lecturer in Law, University of Sheffield
15. Michael Byers, Professor & Canada Research Chair in Global Politics and International Law, University of British Columbia

16. Nicolás Carrillo Santarelli, Associate Researcher, Institute of Human Rights at Business, UDEM University of Monterrey
17. Alejandro Chehtman, Professor of Law, Universidad Torcuato Di Tella (Argentina)
18. Roger S. Clark, Board of Governors Professor Emeritus, Rutgers Law School, Camden, New Jersey
19. Antonio Coco, Lecturer in Public International Law, University of Essex and Visiting Fellow at ELAC, University of Oxford
20. Emily Crawford, Professor, The University of Sydney Law School
21. Rebecca Crootof, Assistant Professor of Law, University of Richmond School of Law
22. Federica D'Alessandra, Executive Director of the Oxford Programme on International Peace and Security, Blavatnik School of Government, University of Oxford
23. Jean D'Aspremont, Chair in Public International Law, University of Manchester; Professor of International Law, Sciences Po School of Law
24. Tom Dannenbaum, Assistant Professor of International Law, The Fletcher School of Law & Diplomacy, Tufts
25. Margaret M. deGuzman, James E. Beasley Professor of Law, Temple University Beasley School of Law
26. François Delerue, Senior Researcher in Cybersecurity Governance, Leiden University
27. Diane A. Desierto, Professor of Law and Global Affairs, Faculty Director of LLM Program in International Human Rights, Notre Dame Law School and Keough School of Global Affairs, University of Notre Dame (USA)
28. Talita Dias, Shaw Foundation Junior Research Fellow, Jesus College; Research Fellow, ELAC, University of Oxford
29. William S. Dodge, Martin Luther King, Jr. Professor of Law and John D. Ayer Chair in Business Law, University of California, Davis, School of Law
30. Jessica Dorsey, Assistant Professor of International and European Law, Utrecht University School of Law
31. Max du Plessis, Senior Counsel and Barrister, South Africa, Adjunct Professor, University of Cape Town and Nelson Mandela University
32. Pavan Duggal, Chairman, International Commission on Cyber Security Law; Founder-cum-Honorary Chancellor, Cyberlaw University; Advocate, Supreme

Court of India

33. Jeffrey L. Dunoff, Laura H. Carnell Professor of Law, Temple University Beasley School of Law
34. Kristen E. Eichensehr, Martha Lubin Karsh and Bruce A. Karsh Bicentennial Professor of Law, University of Virginia School of Law
35. Martin Faix, Senior Lecturer in International Law, Palacký University Olomouc/ Charles University in Prague
36. Tom Farer, Dean Emeritus and University Professor, Josef Korbel School of International Studies, University of Denver
37. David P. Fidler, Senior Fellow for Cybersecurity and Global Health, Council on Foreign Relations (USA)
38. Malgosia Fitzmaurice, Professor of International Law, Queen Mary University of London
39. Micaela Frulli, Professor, Law Department, DSG, Università di Firenze
40. Geoff Gilbert, Professor of International Human Rights & Humanitarian Law, School of Law and Human Rights Centre, University of Essex
41. Chiara Giorgetti, Professor of Law, Richmond Law School, Richmond (VA,USA)
42. Richard J. Goldstone, Retired Justice of the Constitutional Court of South Africa, former Chief Prosecutor of the ICTY and ICTR
43. Guy S. Goodwin-Gill, Professor, Faculty of Law & Justice, University of New South Wales (UNSW); Andrew & Renata Kaldor Centre for International Refugee Law, UNSW; Emeritus Fellow, All Souls College, Oxford
44. Gregory S. Gordon, Professor of Law, The Chinese University of Hong Kong Faculty of Law
45. James A. Green, Professor of Public International Law, Head of Research, Bristol Law School, UWE Bristol
46. Douglas Guilfoyle, Associate Professor of International and Security Law, University of New South Wales Canberra
47. Oleg Gushchyn, Professor, Military Law Department, Taras Shevchenko National University of Kyiv, Ukraine
48. Yael Vias Gvirsman, Director of the International Criminal and Humanitarian Law Clinic, Harry Radzyner Law School, Reichman University, Attorney and Consultant specializing in International Law
49. Steven Haines, Professor of Public International Law, University of Greenwich

50. Monica Hakimi, James V. Campbell Professor of Law, University of Michigan Law School
51. Adil Haque, Professor of Law and Judge Jon O. Newman Scholar, Rutgers Law School
52. Mohamed S. Helal, Associate Professor of Law, The Ohio State University; Member, Permanent Court of Arbitration; Member, African Union Commission on International Law
53. Kevin Jon Heller, Professor of International Law and Security, University of Copenhagen (Centre for Military Studies); Professor of Law, Australian National University
54. Christian Henderson, Professor of International Law, University of Sussex
55. Stacey Henderson, Lecturer, Adelaide Law School, The University of Adelaide
56. Duncan B. Hollis, Laura H. Carnell Professor of Law, Temple University School of Law
57. María José Cervell Hortal, Professor of Public International Law and International Relations, University of Murcia, Spain
58. Deborah Housen-Couriel, The Federmann Cyber Security Research Center at the Hebrew University of Jerusalem; Chief Legal Officer and VP Regulation at Konfidas Digital Ltd
59. Karen Hulme, Professor of Law, University of Essex, United Kingdom
60. Eric Talbot Jensen, Robert W. Barker Professor of Law, Brigham Young University
61. Derek Jinks, A.W. Walker Centennial Chair in Law, University of Texas School of Law
62. Kate Jones, Associate Fellow, Chatham House
63. Ido Kilovaty, Associate Professor of Law, University of Tulsa College of Law
64. Pierre Klein, Professor, Université libre de Bruxelles
65. Robert Kolb, Professor of Public international law, University of Geneva
66. Leonhard Kreuzer, Research Fellow, Max Planck Institute for Comparative Public Law and International Law, Heidelberg, Germany
67. Joanna Kulesza, tenured Professor of International Law and Internet Governance, University of Lodz, Poland
68. Masahiro Kurosaki, Associate Professor of International Law and Director of the Study of Law, Security and Military Operations, National Defense Academy of Japan

69. Henning Lahmann, Hauser Global Postdoctoral Fellow, NYU School of Law
70. Eliav Lieblich, Professor of Law, Buchmann Faculty of Law, Tel Aviv University
71. Noam Lubell, Professor of International Law, Director of the Essex Armed Conflict and Crisis Hub, School of Law & Human Rights Centre, University of Essex
72. Asaf Lubin, Associate Professor of Law, Indiana University Maurer School of Law; Faculty Associate, Berkman Klein Center for Internet and Society, Harvard Law School; Affiliated Fellow, Information Society Project, Yale Law School
73. Fabrizio Marrella, Full Professor of International Law and Vice Rector for International Relations and International Cooperation, "Ca' Foscari" University of Venice, Italy; Professeur invité, Sorbonne Law School
74. Errol P. Mendes, Full professor of constitutional and international law, University of Ottawa, Canada; President, International Commission of Jurists, Canadian Section
75. Marcin J. Menkes, Professor, Warsaw School of Economics
76. Tomohiro Mikanagi, Ministry of Foreign Affairs, Japan
77. Marko Milanovic, Professor of Public International Law, University of Nottingham School of Law
78. Tal Mimran, Adjunct Lecturer, Hebrew University
79. Lindsay Moir, Professor of International Law, University of Hull Law School
80. Evgeni Moyakine, Assistant Professor, Section IT Law / STeP Research Group, Faculty of Law, University of Groningen
81. Harriet Moynihan, Acting Director, International Law Programme, Chatham House (Royal Institute of International Affairs)
82. Roda Mushkat, Professor of International Law, Johns Hopkins University, Paul H. Nitze School of Advanced International Studies (SAIS)
83. James C. O'Brien, Vice-Chair, Albright Stonebridge Group
84. Mary Ellen O'Connell, Robert and Marion Short Professor of Law and Research Professor of International Dispute Resolution, Kroc Institute for International Peace Studies, University of Notre Dame
85. Roger O'Keefe, Professor of International Law, Bocconi University
86. Stefan Oeter, Professor of public International Law and Director of the Institute of International Affairs, Faculty of Law, University of Hamburg
87. Obiora C. Okafor, Edward B. Burling Chair in International Law and Institutions,

School of Advanced International Studies, Johns Hopkins University, Washington DC, USA

88. Inger Österdahl, Professor in Public International Law, Faculty of Law, Uppsala University
89. Bruce Oswald, Professorial Fellow, Melbourne Law School, University of Melbourne
90. Sejal Parmar, Lecturer, School of Law, University of Sheffield
91. Jordan J. Paust, Professor Emeritus, University of Houston Law Center
92. Alison Pert, Adjunct Assistant Professor, The University of Sydney Law School
93. Anni Pues, Lecturer in International Law, Glasgow Centre for International Law and Security, University of Glasgow
94. José Antonio Moreno Rodríguez, Arbitrator, Permanent Court of Arbitration; Member, Inter-American Juridical Committee of the Organization of American States
95. Przemysław Roguski, Lecturer in Law, Jagiellonian University in Kraków, Poland
96. Barrie Sander, Assistant Professor, Leiden University - Faculty of Governance and Global Affairs
97. Andrew Sanger, University Lecturer in International Law, University of Cambridge
98. Marco Sassòli, professor of international law, University of Geneva, Switzerland
99. Ben Saul, Challis Chair of International Law, The University of Sydney
100. Sergey Sayapin, Associate Professor and Associate Dean, School of Law, KIMEP University, Kazakhstan
101. David J. Scheffer, Former U.S. Ambassador at Large for War Crimes Issues; Clinical Professor Emeritus and Director Emeritus, Center for International Human Rights, Northwestern University Pritzker School of Law
102. Michael N. Schmitt, Professor of International Law at the University of Reading and G. Norman Lieber Distinguished Scholar at the United States Military Academy (West Point)
103. Bruno Simma, former Judge at the International Court of Justice; Judge, Iran-United States Claims Tribunal
104. David Sloss, John A. and Elizabeth H. Sutro Professor of Law, Santa Clara University School of Law
105. Lucía Solano, Legal Adviser to the Permanent Mission of Colombia to the United

Nations in New York

106. Alfred H. A. Soons, Professor emeritus of public international law, Utrecht University School of Law, The Netherlands
107. Professor Surya P. Subedi, QC, OBE, DC, Professor of International Law, University of Leeds, and Barrister, Three Stone Chambers, Lincoln's Inn, London
108. Arun Mohan Sukumar, PhD Candidate and pre-doctoral research fellow, Centre for International Law and Governance, The Fletcher School, Tufts University
109. Patrick C. R. Terry, Dean and Professor of Law, University of Public Administration Kehl
110. Kimberley Trapp, Professor of Public International Law, University College London
111. Nicholas Tsagourias, Professor of International Law, University of Sheffield
112. Tsvetelina van Benthem, Lecturer in International Law, Oxford Diplomatic Studies Programme; Research Officer, ELAC, University of Oxford
113. Larissa van den Herik, Professor of Public International Law, Grotius Centre for International Legal Studies, Leiden University
114. Willem van Genugten, Professor em. of International Law, Tilburg University, The Netherlands
115. Liis Vihul, Founder and CEO, Cyber Law International
116. Michael Waibel, Professor of International Law, University of Vienna, Austria
117. Christopher Waters, Professor, Faculty of Law, University of Windsor
118. Philippa Webb, Professor of Law, King's College London
119. Alexander Wentker, Research Fellow, Max Planck Institute for Comparative Public Law and International Law, Heidelberg, Germany
120. Steven Wheatley, Professor of International Law, University of Lancaster
121. Jan Wouters, Full Professor of International Law and International Organizations, Jean Monnet Chair ad personam, Director Leuven Centre for Global Governance Studies – Institute for International Law, KU Leuven
122. Pål Wrange, Professor of Public International Law, Stockholm University, and Director of the Stockholm Centre for International Law and Justice (SCILJ)

THE OXFORD PROCESS

Team

Dapo Akande

Co-Convenor, The Oxford Process
Professor of Public International Law, Blavatnik School of Government; Co-Director and Co-Founder, ELAC

Duncan Hollis

Co-Convenor, The Oxford Process
Laura H. Carnell Professor of Law, Temple Law School

Harold Hongju Koh

Sterling Professor of International Law, Yale Law School

Antonio Coco

Lecturer, Essex Law School
Visiting Scholar, ELAC

Talita Dias

Junior Research Fellow, Jesus College
Research Fellow, ELAC

Priya Urs

Junior Research Fellow, St John's College
Research Fellow, ELAC

Tsvetelina van Benthem

Lecturer in International Law, Oxford Diplomatic Studies Programme
Research Officer, ELAC

THE OXFORD PROCESS

BLAVATNIK SCHOOL OF GOVERNMENT

UNIVERSITY OF OXFORD

OXFORD INSTITUTE FOR ETHICS, LAW AND ARMED CONFLICT