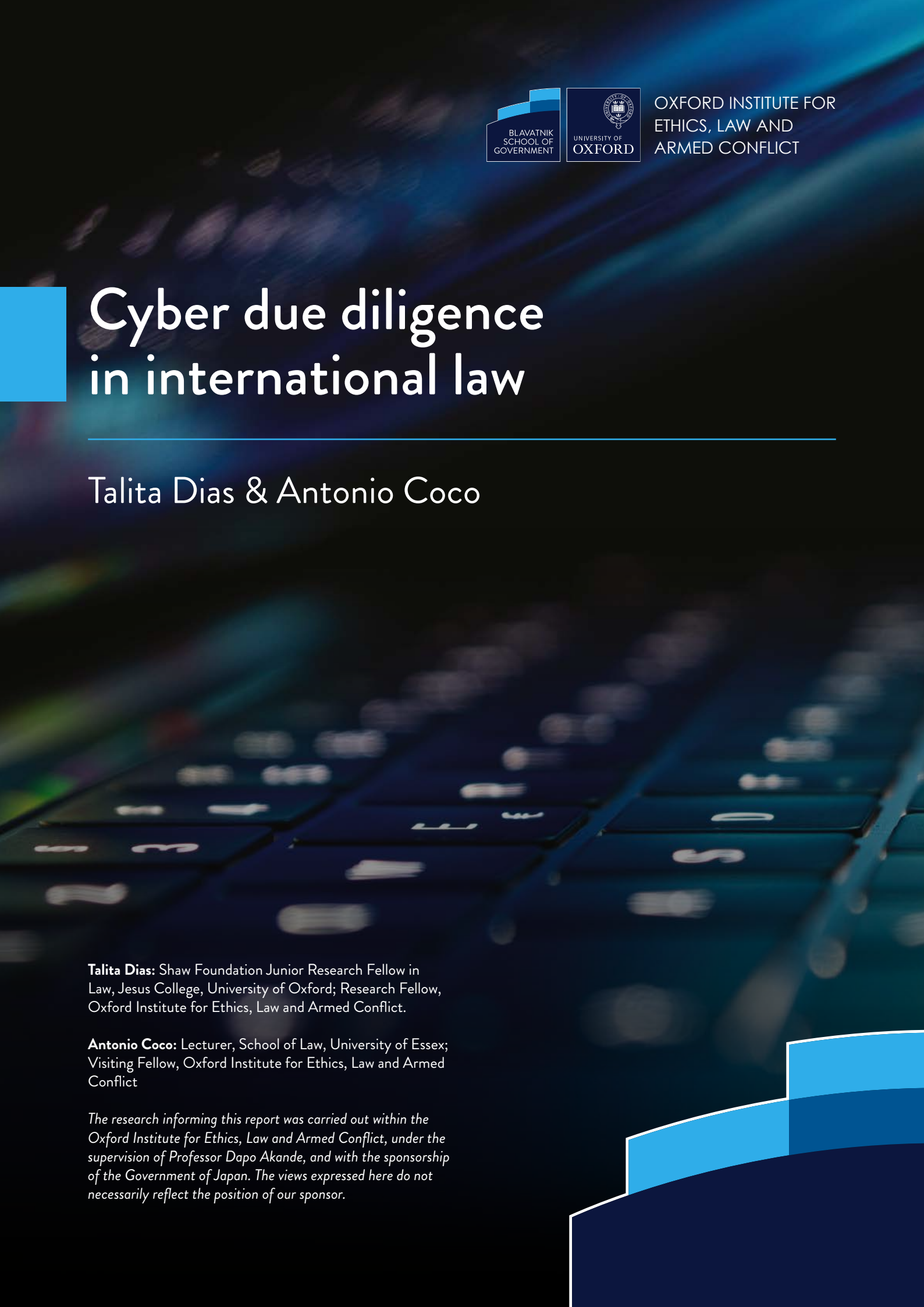

BLAVATNIK SCHOOL OF GOVERNMENT

UNIVERSITY OF OXFORD

OXFORD INSTITUTE FOR ETHICS, LAW AND ARMED CONFLICT

Cyber due diligence in international law

Talita Dias & Antonio Coco

Talita Dias: Shaw Foundation Junior Research Fellow in Law, Jesus College, University of Oxford; Research Fellow, Oxford Institute for Ethics, Law and Armed Conflict.

Antonio Coco: Lecturer, School of Law, University of Essex; Visiting Fellow, Oxford Institute for Ethics, Law and Armed Conflict

The research informing this report was carried out within the Oxford Institute for Ethics, Law and Armed Conflict, under the supervision of Professor Dapo Akande, and with the sponsorship of the Government of Japan. The views expressed here do not necessarily reflect the position of our sponsor.

Contents

Contents continued

Contents continued

Acknowledgements

First and foremost, we are immensely grateful to the Government of Japan, especially Tomohiro Mikanagi, for having given us the opportunity to work on this project. The extent to which international law requires states to behave diligently in cyberspace is not only a fascinating academic topic but also one with significant practical implications for states, private entities and individuals alike. Though many questions remain, this study has opened our eyes to new horizons and spurred further research on that topic. None of this would have been possible without their initiative and constant support.

We also have no words to express our gratitude to our project supervisor and academic mentor, Professor Dapo Akande. These have been difficult times, during which most of this research was carried out remotely. Yet his thoughtful and clear light has guided us through the dark and turbulent sea of solitude. We are particularly thankful for his insightful comments on the various draft chapters of this report, and for his leadership in the workshops we organised.

Special thanks also go to our friend and colleague Tsvetelina van Benthem for her help in making sense of the thorny issues dealt here and her tireless support throughout all project meetings and workshops.

We are thankful to our Research Assistant Leena van Surell for her invaluable comments on individual chapters and her help in putting this final report together.

Last but not least, we wanted to say thank you to all the scholars and practitioners who participated and collaborated with us in the workshops we held throughout this project. We are particularly grateful to the organisers of the Symposium on “Exploring the Frontiers of International Law in Cyberspace”, Dr Przemysław Roguski and Dr Marcin Menkes, whose feedback on earlier versions of Chapter 4 was instrumental. We are also grateful for the support and comments we received from Professors Duncan B. Hollis and Harold Hongju Koh.

Any errors contained in this report remains, of course, our own.

Introduction

Introduction

Due diligence has become a buzz word when it comes to states' use of 'information and communications technologies (ICTs), most prominent among which is the Internet and its numerous applications. The renewed interest in the concept can be explained by the persistent challenges of factually and legally attributing malicious cyber operations to states or even non-state actors. Anonymising and rerouting techniques, such as Virtual Private Networks (VPNs) and other IP (Internet Protocol) spoofing software have compounded the attribution problem, making it difficult if not impossible to trace the origin of a cyber operation.[1] In this context, due diligence features as a promising route to increase peace, security and stability in the ICT environment. This is so to the extent that it might require 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, irrespective of who or what caused them and the legality of the activity in question. For instance, during the COVID-19 pandemic, there have been reports of increased cyber operations targeting the healthcare sector, including hospitals and vaccine research and development facilities.[2] Even though it is difficult to pinpoint who exactly is behind such acts, member states of the European Union 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'.[3]

1 Russel Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm', 21 *Journal of Conflict & Security Law* (2016) 429, at 432.

2 European Union Agency for Cybersecurity (ENISA), 'Cybersecurity in the healthcare sector during COVID-19 pandemic', 11 May 2020, available at https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-healthcare-sector-during-covid-19-pandemic; Menaka Muthuppalaniappan and Kerrie Stevenson, 'Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health,' 33 *International Journal for Quality in Health Care* (2021), 1-4.

3 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 Herczyski, Managing Director for CSDP and Crisis Response, European External Action Service', 22 May 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 'Joint statement from Denmark, Finland, Iceland, Sweden and Norway by Ambassador Mona Juul at the Arria-meeting on Cyber stability and conflict prevention', 22 May 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 Poland, 'Statement by H.E. Tadeusz Chomicki Ambassador for Cyber & Tech Affairs Ministry of Foreign Affairs', 22 May 2020, available at https://vm.ee/sites/default/files/Estonia_for_UN/statement_of_poland_arria_un_sc_on_cyber_22.05.2020.pdf, at 1; and 'Italy's statement at the Arria Formula Meeting on Cyber Stability, Conflict Prevention and Capacity Building', 22 May 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,

Introduction

Yet controversy remains as to whether states are bound by an obligation to behave diligently in their use of ICTs or in what is often called 'cyberspace'. These are multifaceted digital technologies with physical, logical, content and personal dimensions.[4] Notably, the 2015 report by the United Nations (UN) Group of Governmental Experts (GGE) on cybersecurity, adopted by consensus by the UN General Assembly,[5] indicates that States '*should* not knowingly allow their territory to be used for internationally wrongful acts using ICTs'.[6] The provision is explicitly framed as a 'voluntary, non-binding norm' of responsible state behaviour in cyberspace. Nevertheless, 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.[7] According to Rule 6 of the Manual, a state must '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.'[8] On their face, these views seem irreconcilable and neither of them has gone unchallenged.[9]

vaccine and research facilities, as well as electoral processes. On this, see Oxford Institute for Ethics Law and Armed Conflict (ELAC), 'The Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector', 21 May 2020 available at https://elac.web.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea; ELAC, 'The Second Oxford Statement on International Law Protections of the Healthcare Sector During Covid-19: Safeguarding Vaccine Research', 7 August 2020, available at https://elac.web.ox.ac.uk/article/the-second-oxford-statement#/; ELAC, 'The Oxford Statement on International Law Protections Against Foreign Electoral Interference Through Digital Means', 27 October 2020, available at https://elac.web.ox.ac.uk/the-oxford-statement-on-international-law-protections-against-foreign-electoral-interference-through#/. See also ELAC, 'The Oxford Process on International Law Protections in Cyberspace, 2021, available at https://elac.web.ox.ac.uk/the-oxford-process-on-international-law-protections-in-cyberspace#/.

4 Clare Sullivan, 'The 2014 Sony Hack and the Role of International Law', 8 *Journal of National Security Law and Policy* (2015) 437, at 454, fn 88. See also Nicholas Tsagourias, 'The Legal Status of Cyberspace', in Nicholas Tsagourias and Russel Buchan (eds.), *Research Handbook on International Law and Cyberspace* (2015) 13. See also David Johnson and David Post, 'Law and Borders: The Rise of Law in Cyberspace', 48 *Stanford Law Review* (1996) 1367.

5 UN General Assembly, 'Developments in the field of information and telecommunications in the context of international security', GA Res. 70/273, 30 December 2015, paras 1-2(a).

6 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/70/174, 22 July 2015 ('UN GGE Report 2015'), para 13(c).

7 Michael Schmitt (ed.), *Tallinn Manual 2.0* on the International Law Applicable to Cyber Operations (Cambridge University Press, 2017), at 30, Rule 6, and at 43, Rule 7.

8 *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.

9 For instance, Jensen and Watts are cautious about the 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

Introduction

This excessive focus on the legal nature and status of 'due diligence' has resulted in binary, 'all-or-nothing' views: either consensus has been reached about what is 'cyber due diligence' or there would be a legal gap in protection, i.e. states would have no binding obligations but only voluntary undertakings to behave diligently in their use of ICTs. The confusion partly stems from the inconsistent use of the label 'due diligence' as a general principle of law or international law, one or more state obligations, or a standard of behaviour applying in different areas of international law.[10]

To avoid those confusions and contradictions, this Report shifts the debate from label to substance. Rather than simply inquiring whether 'due diligence' applies in cyberspace, its overarching question is: to what extent are states required under international law to protect other states and individuals from harm caused by cyber operations?

In answering this question, this Report begins in Chapter 1 by addressing a preliminary point: how much of international law applies to states' use of ICTs? This chapter challenges the common assumption that, for international legal rules to apply in 'cyberspace', one must produce evidence of state practice and *opinio juris* specifically relating to the 'cyber domain'. It does so by demonstrating that: a) general international law is, by its own nature, generally applicable to all types of state activity, unless a limitation is explicitly stated; b) the notion of 'domain' does not seek to exclude conduct from the scope of otherwise

respect to the supposed burden that the UN GGE Recommendation would impose on States, making them wary to accept it, see Liisi Adamson, 'Recommendation 13(c)', in UN Office of Disarmament Affairs (UNODA), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary* (2017) 49, at 55, para 12. At least three States (Argentina, Israel, New Zealand) have expressed scepticism about the rule: see '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]', 11 February 2020, available at http://webtv.un.org/search/4th-meeting-open-ended-working-group-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-second-substantive-session-10%E2%80%9314-february-2020/6131734500001/?term=%22Open%20Ended%20Working%20Group%22&lan=English&cat=Meetings%2FEvents&sort=date, timestamp 2:15:00; Roy Schondorf, 'Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations', *EJIL:Talk!*, 9 December 2020, available at https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/; and, though in a less clear-cut way, New Zealand Ministry for Foreign Affairs and Trade, 'The Application of International Law to State Activity in Cyberspace', 01 December 2020, paras 16-17., on file with authors. See also Michael Schmitt, 'New Zealand Pushes the Dialogue on International Cyber Law Forward', *Just Security*, 8 December 2020, available at https://www.justsecurity.org/73742/new-zealand-pushes-the-dialogue-on-international-cyber-law-forward/.

10 See Neil McDonald, 'The Role of Due Diligence in International Law', 68 *International and Comparative Law Quarterly* (2019) 1041, at 1043–1044, fn 13; Timo Koivurova, 'Due Diligence', *Max Planck Encyclopaedia of Public International Law (MPEPIL)*, February 2020, available at opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1034?prd=EPIL, paras 1-2 (referring to due diligence as 'an obligation of conduct' as well as a 'concept' and a 'general principle of law').

Introduction

applicable international law; c) 'cyberspace' is not a separate domain, but a set of digital technologies that pervade all traditional domains of land, air, sea and outer space; d) written and unwritten international legal rules may be interpreted to apply to those technologies; because e) international law is technology-neutral, and f) irrespective of any policy recommendations mirroring existing rules or principles. Thus, we conclude that international law applies, as a whole and by default, to ICTs, including when it comes to requiring states to prevent, halt and redress harm.

Next, Chapter 2 seeks to identify the different types of harms of concern to states in the ICT environment. For this purpose, it first explains how the different ICT layers, i.e. software, hardware, data and persons, may be variously affected by harmful cyber operations conducted by states or non-state actors around the world. This chapter then devises a classification of 'cyber harms', depending on the layer and respective attributes affected: whereas software, hardware and data may have their confidentiality, integrity or availability compromised, natural or legal persons may suffer tangible or non-tangible harm. Different types of malicious cyber operations, such as Distributed Denial of Service attacks, ransomware, computer viruses and information operations, are subsequently assessed, focussing on the damage that they may cause to states, non-state groups and individuals. Lastly, this chapter concludes by laying out possible scenarios in which cyber harms may implicate states and non-state actors.

Before turning to the concept of due diligence and the extent to which it applies to ICTs, Chapter 3 briefly discusses how two foundational concepts, namely, state sovereignty and jurisdiction, play out in cyberspace. Indeed, due diligence is a corollary of states' sovereignty over their territory and other areas over their control, and it extends as far as states have jurisdiction to legislate, adjudicate and enforce under international law.[11] This chapter concludes that sovereignty and jurisdiction are better seen under a functional lens, i.e. as concepts that seek to ensure the peaceful coexistence of states and the well-being of

11 *Island of Palmas Case (or Miangas), United States v Netherlands*, Award, 4 April 1928, II RIAA 829 (1928), ICGJ 392 (PCA 1928), at 838.

Introduction

human beings. Accordingly, sovereignty is not only a source of power but also imposes on states duties to act to protect other states and individuals, as well as to tolerate lawful interference resulting from the lawful exercise of jurisdiction in fulfilling those duties.

In what is this Report's main contribution to the international legal debate on 'cyber due diligence', Chapter 4 maps out four sets of protective duties requiring states to prevent, halt or redress certain harms by behaving diligently in their use of ICTs. Two of these can be traced to primary obligations of general 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, articulated in the *Corfu Channel* case,[12] which we call the 'Corfu Channel' principle;[13] b) states' duty to prevent and remedy significant transboundary harm, even if caused by lawful activities, known as the 'no-harm' principle.[14] 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 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. Chapter 4 locates the legal basis of each of those primary rules in customary or conventional international law, unpacks the various standards of due diligence they enshrine and explore the extent to which they apply to States' use of ICTs. This chapter concludes that whether or not a general principle of due diligence applies to ICTs or a binding, cyber-specific 'due diligence rule' exists, states continue to be bound by a patchwork of duties to prevent, stop and redress harm under customary or conventional international law which apply by default to ICTs.

12 *Corfu Channel Case* (*United Kingdom v Albania*), Judgment, 9 April 1949, ICJ Reports (1949) 4, at 22.

13 August Reinisch and Markus 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* (2015) 101, at 106.

14 See *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.

Introduction

This Report ends with Chapter 5, which looks at how the various protective international obligations requiring 'diligent state behaviour' in the ICT environment have been and ought to be implemented in practice. Specifically, this chapter starts by looking at current trends with regards to states' behaviour and attitudes in their use of ICTs to confirm that existing international legal rules containing a standard of due diligence apply to those technologies. The chapter goes on to draw specific guidance for the implementation of those rules from a representative survey of states' laws, policies and views on ICTs. States surveyed include Japan, China, Singapore, Russia, the United Kingdom, Germany, France, the United States, Canada, Brazil, Argentina, South Africa, Iran and Australia. This survey supports the conclusion that states may comply with their various protective obligations in the ICT environment by adopting a wide variety of legal, technical, organisational, capacity-building and cooperative measures.

Altogether, the findings laid out in this Report point to one overarching conclusion: though not a silver bullet against all cybersecurity challenges, the international legal 'patchwork' of protective duties enshrining a standard of due diligence *already* plays a central role in the pursuit of a more peaceful, secure and stable ICT environment. The paramount importance and implications of diligent state behaviour in the use of today's and tomorrow's ICTs should be further disseminated and acknowledged by governments, the private sector, academia and civil society.

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

1. Introduction

The applicability of existing international law to cyberspace has received widespread support among states. It has been recognised by individual governments as well as in the 2013[1] and 2015[2] reports by the United Nations (UN) Group of Governmental Experts (GGE) on information and communications technologies (ICTs), both of which were endorsed by the UN General Assembly by consensus.[3] More recently, the Final Substantive Report of the UN Open-ended working group on developments in the field of information and telecommunications in the context of international security (OEWG), also adopted by consensus among all UN member states, 'reaffirmed that international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace, security and stability in the ICT environment.'[4] A similar statement is found in the latest GGE report, adopted in May 2021.[5]

In particular, there is agreement that 'sovereignty and international norms and principles that flow from sovereignty' apply to states' ICT-related activities and their jurisdiction over ICT infrastructure within their territory.[6] Likewise, states have explicitly endorsed the applicability of the UN Charter in its entirety, along with fundamental principles such dispute settlement by peaceful means and non-intervention.[7] States have also recognised that they must respect and

1 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'), para 19.

2 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'), paras 24 and 28(a).

3 GA Res. 70/237, 30 December 2015, paras 1-2(a).

4 OEWG, Final Substantive Report, UN Doc A/AC.290/2021/CRP.2, 10 March 2021 ('OEWG Final Substantive Report'), para 7.

5 Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, Advance Copy, 28 May 2021) (hereinafter UN GGE Report 2021), available at https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf, para 69.

6 UN GGE Report 2013, *supra* note 1, para 20; UN GGE Report 2015, *supra* note 2, para 27; UN GGE Report 2021, *supra* note 5, para 71(b).

7 UN GGE Report 2013, *supra* note 1, para 20; UN GGE Report 2015, *supra* note 2, paras 25-28; UN GGE Report 2021, *supra* note 5, paras 70, 71(a) and (e).

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

protect human rights and fundamental freedoms and, where applicable, the principles of humanity, necessity, proportionality and distinction.[8] More generally, they have committed 'to meet[ing] their international obligations regarding internationally wrongful acts attributable to them under international law',[9] as well as to not using proxies to commit such acts.[10]

However, the full extent to which international law applies to ICTs has not been spelled out in the 2015 and 2013 GGE reports, in the OEWG Final Substantive Report, or in some individual government statements. This uncertainty has led some states and scholars to question the applicability of certain international rules and principles in 'cyberspace'. This is the case of sovereignty *as a rule* capable of being breached, whose applicability to cyberspace has been opposed by the United Kingdom (UK).[11] Similarly, the applicability of International Humanitarian Law (IHL) as a whole has been questioned by states such as Russia[12] and China.[13] Crucially, the concept of due diligence as a binding rule or principle of international law applicable to cyberspace

8 UN GGE Report 2013, *supra* note 1, para 21; UN GGE Report 2015, *supra* note 2, paras 26 and 28(b) and (d); UN GGE Report 2021, *supra* note 5, paras 70, 71(f).

9 UN GGE Report 2013, *supra* note 1, para 23; UN GGE Report 2015, *supra* note 2, para 28(f); UN GGE Report 2021, *supra* note 5, para 71(g).

10 UN GGE Report 2013, *supra* note 1, para 23; UN GGE Report 2015, *supra* note 2, para 28(e); UN GGE Report 2021, *supra* note 5, para 71(g).

11 'Cyber and International Law in the 21st Century, Speech by United Kingdom Attorney General Jeremy Wright QC MP', 23 May 2018, available at https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century ('UK 2018 Speech'), at 5; UK Mission to the United Nations, 'United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security: Application of International Law To States' Conduct In Cyberspace – United Kingdom Statement', 3 June 2020, available at https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement, para 10.

12 'Statement by Minister-Counsellor Mr. Yao Shaojun at Arria Formula Meeting on Cyber Attacks Against Critical Infrastructure', 26 August 2020, available at https://www.fmprc.gov.cn/ce/ceun/eng/hyyfy/t1809700.htm; 'Statement by Chinese representative during UNSC Arria Formula Meeting on Cybersecurity', 22 May 2020, available at https://vm.ee/en/activities-objectives/estonia-united-nations/signature-event-estonias-unsc-presidency-cyber, at timestamp 1:21:00.

13 'Commentary of the Russian Federation on the Initial "Pre-Draft" of the Final Report of the United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security', 22 May 2020, available at https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf, at 2.

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

has been explicitly rejected by Argentina[14] and Israel,[15] and seriously questioned by New Zealand,[16] and the UK.[17] To compound the uncertainty, a majority of states have not yet expressed their views on the status of due diligence in international law or its applicability to cyberspace.

Arguments that deny the applicability of due diligence or other existing rules or principles of international law to cyberspace usually rest on three related assumptions. First, it is often said that cyberspace is a new and inherently different 'space', 'field' or 'domain' of state activity. Accordingly, like the physical domains of air, land, sea and outer space, the 'cyber domain', although virtual, would require specifically tailored rules or principles of international law. Second, it follows that existing international law could only apply '*in* cyberspace' if substantiated by sufficient evidence of domain-specific state practice and *opinio juris*.[18] This search for cyber-specific practice and *opinio juris* is usually backed with calls for more national statements on how international law applies to cyber operations. Third, the fact that certain standards of conduct have been framed, in the 2015 UN GGE Report, as 'voluntary, non-binding, norms of responsible state behaviour in cyberspace', is taken to mean that the behaviour in question is not required by international law.

This is precisely the case of the concept of due diligence, which seems to be reflected in both UN GGE Reports in hortatory terms: '[s]tates *should* not knowingly allow their territory to be used for internationally

14 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], 11 February 2020 ('Argentina's Intervention at the 2nd Substantive GGE Meeting'), available at http://webtv.un.org/search/4th-meeting-open-ended-working-group-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-second-substantive-session-10%E2%80%9314-february-2020/6131734500001/?term=%22Open%20Ended%20Working%20Group%22&lan=English&cat=Meetings%2FEvents&sort=date, timestamp 2:15:00.

15 Roy Schondorf, 'Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations', EJIL: Talk!, 9 December 2020, available at https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/.

16 New Zealand Ministry for Foreign Affairs and Trade, 'The Application of International Law to State Activity in Cyberspace', 01 December 2020, paras 16-17., on file with authors. See also Michael Schmitt, 'New Zealand Pushes the Dialogue on International Cyber Law Forward', *Just Security*, 8 December 2020, available at https://www.justsecurity.org/73742/new-zealand-pushes-the-dialogue-on-international-cyber-law-forward/.

17 UK Mission to the United Nations, *supra* note 11, para 12.

18 *Ibid*, paras 10 and 12.

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

wrongful acts using ICTs' or 'should seek to ensure that their territory is not used by non-State actors to commit such acts'.[19] For some, the implication of labelling a standard of conduct as a 'voluntary, non-binding, norm', or framing it as something that states 'should' endeavour to achieve, 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.[20]

This set of arguments finds its clearest expression in the recent statement by Israel's Deputy Attorney General on the application of international law to cyber operations:[21]

> 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.

With specific regards to the concept of due diligence, the statement goes on to posit that:[22]

> There was wisdom in mentioning [due diligence] in the chapter covering norms of responsible State behavior, as it does not, at this point in time, translate into a binding rule of international law in the cyber context. [...]

19 UN GGE Report 2013, *supra* note 1, para 23; UN GGE Report 2015, *supra* note 2, para 13(c); UN GGE Report 2021, *supra* note 5, paras 29-30.

20 E.g., UK Mission to the United Nations, *supra* note 11, para 12.

21 Schondorf, *supra* note 15.

22 Ibid.

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

> As I mentioned regarding the examples of maritime blockade and neutrality, we have to be careful in applying to the cyber domain rules that emerged in a different, distinct context. For instance, in the field of environmental law, where much of the focus and application of due diligence obligations has been in recent years, the acting State typically has control, or at least oversight, over the harmful activity (for example, regulating a polluting power plant). However, cyberspace is mostly private and decentralized.
>
> The inherent different features of cyberspace – its decentralization and private characteristics – incentivize cooperation between States on a voluntary basis, such as with the case of national Computer Emergency Response Teams (CERTs). […] However, we have not seen widespread State practice beyond this type of voluntary cooperation, and certainly not practice grounded in some overarching *opinio juris*, which would be indispensable for a customary rule of due diligence, or something similar to that, to form.

Yet those assumptions may be challenged on at least six different bases which we explore further in this chapter.

First, Section 2 starts by explaining why general international law is *not* domain-specific, in the sense that it only applies, by default, to the traditional domains of land, air and/or sea, and its applicability to other domains must be specifically proven. Quite the contrary: any limitation imposed on the scope of general international law, whether framed around a subject-matter, context, area, type of activity or 'domain', cannot be implied but must be assessed.

Second, and relatedly, Section 3 demonstrates that rules of international law, whether conventional or customary, which evince a general scope of application, can be interpreted and applied to new 'domains'.

Next, Section 4 delves into the notion of 'domain' and its development in the context of international humanitarian law (IHL). We demonstrate that, in this and other areas, the concept was never meant to function as a device to carve out certain types of activity from existing rules or principles of international law.

Section 5 then considers that, in any event, cyberspace is not per se a 'space' or a singular 'domain,' at least not in the sense that air, sea or outer space are. Instead, it is a combination of digital technologies or ICTs spread across national borders and made up of physical, logical and personal elements, just like other technologies, albeit on a different scale.

In the same vein, Section 6 advances that international law is technology-neutral, in the sense that it applies to all technologies through which states and non-state actors operate, whether these are old or new, analogical or digital, physical or virtual.

Lastly, Section 7 contends that the mere fact that a certain behaviour has been the subject of a policy recommendation by no means implies that the same behaviour is not required as a matter of international law. Quite the opposite: political statements cannot deprive international obligations of their binding force.

In what follows, we develop the foregoing points and conclude that due diligence, whether a rule or principle, applies *by default* to ICTs, i.e., 'cyber' operations conducted by states or non-state actors using those technologies.

2. The 'generality' of general international law

That *general* international law is, by definition, general is self-evident. But that does not tell us much about its extent or scope of application, i.e., who is bound by general international and to what matters it applies. For this reason, it is important to grasp the different ways in which international law can be said to 'apply generally', and, in

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

particular, the extent to which this generality includes different subject-matters, contexts, areas or types of activity.

First and foremost, 'general international law' refers to international rules and principles that bind all states as a matter of customary international law, general principles of law or universally ratified treaties.[23] Examples include the principles of sovereign equality of states and non-intervention, as well as the UN Charter and its prohibition on the use of force, binding under conventional and customary international law.[24] Among those rules and principles generally applicable to all states, some deal with more specific matters than others. For instance, the four 1949 Geneva Conventions have been universally ratified and crystallized into customary international law, thereby applying to all states.[25] Yet their subject-matter is limited to regulating the conduct of hostilities during armed conflict, that is, to the so-called 'field' of IHL.[26] Likewise, the principle of non-intervention in the internal affairs of other states, although not limited to situations of armed conflict, only covers coercive interference within another state's '*domaine reservé*', that is, public or private matters which the state exercises exclusive authority to regulate.[27] In fact, apart from a handful of very general and foundational principles of international law, from which states' obligations seem to flow, such as sovereignty and *pacta sund servanda*, international rules and principles tend to have a more or less defined subject-matter.

23 See Josef L. Kunz, 'General International Law and the Law of International Organizations', (1953) 47 *American Journal of International Law* 456, at 456-457; Anastasios Gourgourinis, 'General/Particular International Law and Primary/Secondary Rules: Unitary Terminology of a Fragmented System', 22 *European Journal of International Law* (2011) 993, at 1004-1007; International Law Commission (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, para 493.

24 Art. 2(4), Charter of the United Nations, adopted 24 October 1945, 1 UNTS XVI.

25 See Theodor Meron, 'The Geneva Conventions as Customary Law', 81 *American Journal of International Law* (1987) 348-370.

26 See Common Article 2, Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention), adopted 12 August 1949, entered into force 21 October 1950, 75 UNTS 287.

27 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)*, Judgment, 27 June 1986, ICJ Reports (1987) 14., para 202; UN General Assembly, 'Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations', UN Doc A/RES/2625(XXV), 24 October 1970, Principle 'c'. See also Schmitt, Michael Schmitt (ed.), *Tallinn Manual 2.0* on the International Law Applicable to Cyber Operations (Cambridge University Press, 2017), at 24, Commentary to Rule 4, para 22. But see Harriet Moynihan, 'The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention', Chatham House Research Paper, 2 December 2019, available at https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/3-application-non-intervention-principle, paras 105-107 (advancing a broader scope for the principle).

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

In some instances, explicit or implicit treaty texts or state practice and/or *opinio juris* indicate that the application of an international rule or principle is limited to a particular 'context', area or specific type of activity. This is the case of the centuries-old obligation of states to respect freedom of navigation in the high seas, whose practice and *opinio juris* clearly evince is restricted to the *high* seas.[28] The rule does not guarantee freedom of navigation throughout the seas, nor does it oblige states to guarantee freedom of movement in other maritime zones, such as states' territorial waters or their Exclusive Economic Zones.[29] Similarly, the obligation to carry out an environmental impact assessment, although binding under customary international law, only applies to those activities that may cause physical harm to the natural environment.[30]

Nevertheless, in the absence of a limitation to a particular subject-matter, context, area or type of activity, or where the previous expression of a rule is general (whether its text, or formative *opinio juris* and state practice), there is nothing in international law that suggests that one must seek to ascertain whether a rule applies across 'domains', as many have sought to characterise 'cyberspace' or ICTs. For example, it is prohibited for states to arrest the serving head of another state. It matters not where or how 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 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. This means that we should be sceptical about a supposition that the application of international law rules is 'domain' specific.

28 See Art. 87, United Nations Convention on the Law of the Sea, adopted 10 December 1982, entered into force on 1 November 1994, 1833 UNTS 397; Hugo Grotius, 'The Freedom of the Seas; Or, the Right which Belongs to the Dutch to Take Part in the East Indian Trade' (Oxford University Press, 1916), at 28; Albert J Hoffmann, 'Freedom of Navigation', *MPEPIL*, April 2011, available at https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1199, paras 1-6; Douglas Guilfoyle, 'The High Seas', in Donald Rothwell, Alex Oude Elferink, Karen Scott, and Tim Stephens (eds), *The Oxford Handbook of the Law of the Sea* (Oxford University Press, 2015) 204, at 207.

29 Hoffmann, *ibid*, para 6.

30 See Pulp Mills on the River Uruguay, Case Concerning (Argentina v Uruguay), Judgment, 20 April 2010, ICJ Reports (2010) 14, para 204; Certain Activities Carried out by Nicaragua in the Border Area (Costa Rica v Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v Costa Rica), Judgment, 16 December 2015, ICJ reports (2015) 665, para 104; Astrid Epiney, 'Environmental Impact Assessment', *MPEPIL*, January 2009, available at *https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1581*, paras 1-4.

The bottom-line is that, to ascertain the scope of application of general international law, each rule or principle must be assessed on its own terms. Thus, whether a limitation is based or framed around a subject-matter, a context, an area, a type of activity, a 'domain', or any other category we might conceive of for that matter, it must be somehow indicated in the rule or principle in question. Importantly, to undertake this assessment, traditional methods of *interpretation* of treaties or customary international law, must be resorted to. These methods tell us that, where a rule is *not* limited to a certain area, context, type of activity, or domain, its scope can be interpreted and applied to cover any such category. It is to this point that we now turn.

3. Interpreting and applying general international law to new 'domains'

As outlined earlier, legal interpretation is the most intuitive way to ascertain the scope of a certain rule or principle of conventional or customary international law and any potential 'domain' or other limitation thereto. That treaties must be interpreted in accordance with their text, context and object and purpose is beyond doubt.[31] But much controversy surrounds the interpretability of unwritten rules of international law, including custom and general principles.[32] In what follows, we explain why, in the absence of specific limitations, both written and unwritten rules of international law of *general scope* are susceptible to identification and/or interpretation as well application in the cyber context, i.e. to ICTs.[33] In particular, we tackle the controversial question as to whether it is necessary to prove specific state practice and *opinio juris* for existing rules of international law to apply in cyberspace.

31 Arts. 31-33, Vienna Convention on the Law of Treaties, adopted 23 May 1969, entered into force 27 January 1980, 1155 UNTS 331 (VCLT).

32 ILA, 'Study Group on the Content and Evolution of the Rules of Interpretation, Preliminary Report' (2016), available at http://www.ila-hq.org/download.cfm/docid/4AD3C3F1-D91D-4142-8D192EBFBA4E35B9 ('ILA Study on Interpretation'). See also Robert Kolb, *Interprétation et création du droit international: esquisses d'une herméneutique juridique moderne pour le droit international public* (Bruylant, 2006), at 219-222; Panos Merkouris, 'Interpreting the Customary Rules on Interpretation', (2016) *University of Groningen Faculty of Law Research Paper 2016-12*, available at https://papers.ssrn.com/abstract=2749066; Duncan B Hollis, 'Sources and Interpretation Theories: An Interdependent Relationship' (2016) *Temple University Legal Studies Research Paper No 2016-46*, available at https://papers.ssrn.com/abstract=2836691.

33 Orfeas Chasapis Tassinis, 'Customary International Law: Interpretation from Beginning to End', 31 (2020) *European Journal of International Law* 235, at 236.

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

While the interpretability of customary international law is beyond the scope of this report, it suffices to note that, no matter how international lawyers frame the process or methodology for ascertaining the existence, content and scope of customary international law, there is always room for interpretation in every step of the way.[34] This is because interpretation, understood here as the process of assigning meaning to subjects, objects or events, is inherent to human cognition. Simply put, it is by assimilating specific things to abstract concepts that we understand and communicate about the world around us.[35] And in this process of 'framing', there is inevitably room for over or under-inclusion, at the very least when it comes to man-made, non-deterministic concepts or ideas such as law.[36] Of course, questions remain as to whether it is even possible to separate the stages of identification or ascertainment of state practice and *opinio juris*, and the interpretation of an identified rule of custom.[37] As others have noted, even the exercises of selecting, describing and evaluating state practice and *opinio juris* are pervaded by subjectivity, and are thus subject to different interpretations.[38] Either way, it is sensible to assume that custom or its separate elements are interpretable,[39] i.e. that the original, abstract 'frame' can always be extended to cover new and more specific phenomena.

34 Similarly, ibid, at 237 and 241.

35 Ibid, at 242-243.

36 See ibid, at 244 and Matthias Herdegen, 'Interpretation in International Law', *MPEPIL*, Mach 2013, available at https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e723, para 1.

37 See Tassinis, *supra* note 33, at 246; Hollis, *supra* note 32, at 2, 4-6, 8; Duncan B. Hollis, 'The Existential Function of Interpretation in International Law' in Andrea Bianchi, Daniel Peat and Matthew Windsor (eds), *Interpretation in International Law* (OUP, 2015) 80; Jean D'Aspremont, 'The Multidimensional Process of Interpretation' in Andrea Bianchi, Daniel Peat and Matthew Windsor (eds), *Interpretation in International Law* (Oxford University Press, 2015), at 117-118.

38 Tassinis, *supra* note 33, at 257; Federick Schauer, 'Pitfalls in the Interpretation of Customary International Law', in Amanda Perreau-Saussine, and James B. Murphy, *The Nature of Customary Law: Legal, Historical and Philosophical Perspectives* (Cambridge University Press, 2007), at 21; Nadia Banteka, 'A Theory of Constructive Interpretation for Customary International Law Identification' 39 *Michigan Journal of International Law* (2018) 301, at 316.

39 See North Sea Continental Shelf (Germany v. Denmark and the Netherlands), ICJ Reports (1969) 3, Dissenting Opinion of Judge Tanaka ('Judge Tanaka's Dissent in North Sea'), at 181; Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America), Judgment, 27 June 1986, ICJ Reports (1987) 14, para. 178; European Communities — Measures Affecting the Approval and Marketing of Biotech Products, WTO, Panel Report adopted on 21 November 2006, WT/DS291R, WT/DS292R and WT/DS293R, paras. 7.68-7.72

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

Having established that both treaties and custom are interpretable, the question that arises is whether the concept of due diligence, along with other traditional rules whose applicability to cyberspace has been questioned, is sufficiently wide or general to cover cyber operations - whether these are framed as a new and exceptional domain, area, context or type of activity. And the answer is, quite simply, that there is no evidence that due diligence, or sovereignty and IHL for that matter, are limited to the traditional 'physical' domains of land, air and sea. Rather – and without prejudice to the question of whether due diligence is a rule, a shorthand for various obligations or a general principle – the concept is quite general in scope, as we shall explore further in Chapter 4 below.

The most prominent rule which requires due diligence from states is the general principle articulated in the Corfu Channel case. In this case, the specific question before the ICJ was Albania's duty to notify British vessels of mines which it should have known were placed in its territorial waters. Yet, the Court found that at the source of this particular duty was a more general obligation of every state 'not to allow knowingly its territory to be used for acts contrary to the rights of other States'. Even prior to Corfu, the Arbitral Tribunal in the Island of Palmas case, whilst dealing with the concept of sovereignty and its corollary obligations in the context of a territorial dispute, framed the same duty of prevention as:

> the obligation to protect within the territory the rights of other States, in particular their right to integrity and inviolability in peace and in war, together with the rights which each State may claim for its nationals in foreign territory.[40]

As this passage makes it clear, the longstanding duty to protect the rights of other states within a state's own territory by exercising due diligence is not limited by subject-matter, context, area, or even domain. The same goes for the concept of territorial sovereignty, which, as the same Arbitral Tribunal found, 'is, *in general*, a situation recognized and delimited in space, either by so-called natural frontiers

40 *Corfu Channel Case* (*United Kingdom v Albania*), Judgment, 9 April 1949, ICJ Reports (1949) 4, at 839.

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

[…] or by outward signs of delimitation that are undisputed, or else by legal engagements entered into between interested neighbours.'[41] Even the duty to prevent and redress transboundary harm, known as the 'no-harm' or 'good neighbourliness' principle, discussed in detail in Chapter 4, although more readily associated with the natural environment and ecological matters, applies well beyond this context, as the ILC's comprehensive survey of state practice and *opinio juris* over decades showcases.

An alternative, albeit less natural, way to frame and conceptualise the application of general rules of customary international law to new types of scenarios is as the identification of new customary rules, which are specifically tailored to the situation, context or 'domain' at hand. This is, according to some scholars,[42] what the ICJ did with the more general due diligence principle and Albania's specific duty to notify British vessels about mines in the Corfu Channel.[43] Likewise, this approach seems to have been followed by some states and scholars in relation to a rule of due diligence in cyberspace: it is often assumed that a new and cyber-specific rule of due diligence must be specifically identified and applied to ICTs.[44]

However, and crucially, even if one frames the applicability of international law to new domains as custom-identification or ascertainment, there is usually no need to collate specific instances of state practice and *opinio juris* from scratch by induction. This is because, whenever a more general rule or principle of international law already exists whose scope covers a new situation or domain, it is possible to deduce one or more specific rules from the more

41 Ibid, at 838, emphasis added.

42 See, e.g., Stefan Talmon, 'Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion', 26 *European Journal of International Law* (2015) 417, at 424; Banteka, *supra* note 38, at 303, 311-312.

43 *Corfu Channel*, *supra* note 40, at 22.

44 E.g., Eric Talbot Jensen and Sean Watts, 'A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?', 95 *Texas Law Review* (2017) 1555, at 1573-1574; Schmitt, *Tallinn Manual 2.0*, *supra* note 27, at 45 (referring to the views expressed by some scholars in the Manual's International Group of Experts); Luke Chircop, 'A Due Diligence Standard of Attribution in Cyberspace', 67 *International and Comparative Law Quarterly* (2018) 643, at 660, 662. See also Michael N. Schmitt, '"Virtual Disenfranchisement": Cyber Election Meddling in the Grey Zones of International Law', 19 *Chicago Journal of International Law* (2008) 30, at 20; 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. 615/20 rev.1 7 August 2020 ('Improving Transparency'), para 7 (referring generally to the need for evidence of state practice and *opinio juris* to assess the applicability of international law in cyberspace).

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

general one.[45] As Tassinis notes, this can be explained by the nature of customary international law as 'an organic body of legal rules that gradually branches out as opposed to an assemblage of self-standing rules'.[46] Granted, it may not be that every rule of custom is *directly* rooted in a pre-existing one. This may be the case of certain rules of procedure, such as the requirement that instruments of ratification of treaties be exchanged or deposited with, or notified to the other party(ies).[47] However, all rules of custom are ultimately grounded or at least informed by foundational international legal principles, such as sovereignty, consent and good faith.[48] Although deduction from general rules or principles alone may not always suffice to prove the existence of a more specific rule of custom, it does raise a strong presumption that such a rule does exist, in turn lowering the threshold of state practice and opinio juris which would be necessary to prove its existence.[49] According to Talmon, in those instances, the outcome of the deductive process is simply *confirmed* by induction from a sufficient amount of state practice and *opinio juris*.[50]

In practice, there is little difference between this process of custom-identification and the interpretation and application of general customary rules to new phenomena. Admittedly, it remains unclear what canons of interpretation should be applied to customary international law, whether reflected in textual form or drawn from a set of behaviours.[51] But any type of legal interpretation, whether in domestic or international law, can only be informed by a handful of legal reasoning techniques. As made explicit in the context of treaty interpretation, these include the ordinary meaning of the words by

45 Talmon, supra note 42, at 421-423. See also Anthea Elizabeth Roberts, 'Traditional and Modern Approaches to Customary International Law: A Reconciliation' (2001) 95 *American Journal of International Law* 757, at 758-759; Dapo Akande, 'The Jurisdiction of the International Criminal Court over Nationals of Non-Parties: Legal Basis and Limits' 1 *Journal of International Criminal Justice* (2003) 618, at 626.

46 Tassinis, *supra* note 33, at 262.

47 Art. 11 VCLT 1980.

48 See Banteka, *supra* note 38, at 316.

49 Talmon, *supra* note 42, at 427.

50 Ibid.

51 ILA Study on Interpretation, *supra* note 32, at 9.

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

which a rule is expressed, its context, its function or objective, and its history (textual, systematic, teleological and historical methods of interpretation, respectively).[52] Other methods of interpretation which also apply to written and unwritten legal rules include analogy, *a contrario*, *in dubio mitis*, and other techniques of logical reasoning.[53] That customary international law can be interpreted by these and other techniques has long been acknowledged before human rights bodies and international criminal courts.[54] These have sought to clarify the extent to which more general customary prescriptions or prohibitions apply to specific factual scenarios, often unforeseen at the time the rule was conceived, by using different interpretative techniques.[55] Notably, in various international courts and tribunals, as well as diplomatic settings, a key technique to interpret treaty and customary rules — and trace their evolution over time — is to look at the subsequent practice of states, which implicitly or explicitly establishes their agreement.[56]

In the context of due diligence this means that, whether one chooses to proceed by identifying one or more specific obligations or by interpreting general principles or rules to cover ICTs, the end-result is the same: states *must* behave diligently in cyberspace and other so-called 'domains', as a matter of general international law. That one or more due diligence obligations under international law bind states in cyberspace can be confirmed by current evidence of state practice and *opinio juris*. In fact, not only are statements denying the applicability of due diligence to cyberspace fairly limited – to the

52 Arts. 31-32 VCLT. See also Odile Ammann, Domestic Courts and the Interpretation of International Law Methods and Reasoning Based on the Swiss Example (Brill, 2019), Chapter 6, at 192 ff.

53 Mark E. Villiger, 'The Rules on Interpretation: Misgivings, Misunderstandings, Miscarriage? The "Crucible" Intended by the International Law Commission', in Enzo Cannizzaro (ed.), *The Law of Treaties Beyond the Vienna Convention* (Oxford University Press, 2011), at 112.

54 See, e.g., *Vasiljević*, Judgement, ICTY, Trial Chamber II, 29 November 2002, IT-98-32-T, paras 193, 196, 201-202; *Vasiliauskas v Lithuania*, App no 35343/05 (ECtHR, 20 October 2015), paras 171-186.

55 See, e.g., ECtHR, *Sunday Times v The United Kingdom*, Appl. no 6538/74, Judgement 26 April 1979), para 59; ECtHR, *SW v United Kingdom*, Appl. No 20166/92, Judgement of 22 November 1995, para 36; *Hadzihasanović et al*, Interlocutory Appeal on Decision on Joint Challenge to Jurisdiction, ICTY, Appeals Chamber, 27 November 2002, IT-01-47-PT, para 12.

56 On subsequent practice and customary international law interpretation, see, e.g., *North Sea Continental Shelf (Germany v. Denmark and the Netherlands)*, ICJ Rep (1969) 3, paras 44-56; *Vasiliauskas*, *supra* note 54, paras 176-177. On the role of subsequent practice in the context of treaty interpretation, see Art. 31(3)(c) VCLT; ILC, 'Report on the Work of the Sixty-Eighth Session (2016), 'Chapter VI: Subsequent Agreements and Subsequent Practice in Relation to the Interpretation of Treaties', (2016) A/71/10.

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

four abovementioned statements by Argentina, Israel, the UK and New Zealand – but several states have spoken out in support of the applicability of international law *as a whole* to cyberspace.[57] Even more tellingly, a growing number of states and international organisations, such as France,[58] The Netherlands,[59] Estonia,[60] Finland,[61] Denmark, Iceland, Sweden, Norway,[62] the Czech Republic,[63] the Dominican Republic,[64] Chile, Ecuador, Guatemala, Guyana and Peru,[65] Japan,[66] the Republic of Korea,[67] and the European Union (EU)[68] have explicitly

57 See, e.g., 'Estonian SC Arria Meeting: Cyber Stability, Conflict Prevention and Capacity Building Statement by Austria, delivered by H.E. Mr. Jan Kickert, Permanent Representative of Austria to the United Nations', 22 May 2020, available at https://www.bmeia.gv.at/fileadmin/user_upload/Vertretungen/OEV_New_York/JW/22_May_2020Security_Council_Arria_Formula_Meeting_Cyber_Stability_-_Statement_by_Austria.pdf; 'Pre-Draft Report of the OEWG - ICT: Comments by Austria', 31 March 2020, available at https://front.un-arm.org/wp-content/uploads/2020/04/comments-by-austria.pdf; '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', 11 March 2020 ('Comments by the Czech Republic'), available at https://front.un-arm.org/wp-content/uploads/2020/04/czech-republic-oewg-pre-draft-suggestions.pdf; 'France's response to the pre-draft report from the OEWG Chair', May 2020' ('France's response), available at https://front.un-arm.org/wp-content/uploads/2020/04/contribution-fr-oewg-eng-vf.pdf; 'The Kingdom of the Netherlands' response to the pre-draft report of the OEWG', 1 April 2020, available at https://front.un-arm.org/wp-content/uploads/2020/04/kingdom-of-the-netherlands-response-pre-draft-oewg.pdf.

58 France's response, *supra* note 57; French Ministry of Defence, 'Droit International Appliqué Aux Opérations Dans Le Cyberespace', 9 September 2019, available at https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqué+aux+opérations+Cyberespace.pdf.

59 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, 5 July 2019' ('Netherlands Letter'), 5 July 2019, available at https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace.

60 Estonia, 'President of the Republic at the opening of CyCon 2019', 29 May 2019, available at https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html.

61 'International law and cyberspace: Finland's national positions', 15 October 2020 ('Finland's Position'), available at https://um.fi/documents/35732/0/Cyber+and+international+law%3B+Finland%27s+views.pdf/41404cbb-d300-a3b9-92e4-a7d675d5d585?t=1602758856859.

62 'Joint statement from Denmark, Finland, Iceland, Sweden and Norway by Ambassador Mona Juul at the Arria-meeting on Cyber stability and conflict prevention', 22 May 2020, available at https://www.norway.no/en/missions/UN/statements/security-council/2020/arria-cyber-stability-and-conflict-prevention.

63 Comments by the Czech Republic, *supra* note 57, at 3.

64 'Statement by the Dominican Republic's Ambassador and Special Envoy to the Security Council, H.E. Mr. José Singer Weisinger', 2 May 2020, available at https://vm.ee/sites/default/files/Estonia_for_UN/22-5-2020_cyber_stability_and_conflict_prevention_-3.pdf (Dominican Republic's Statement').

65 OAS, Improving Transparency, *supra* note 44, para 58. See also paras 56ff.

66 Ministry of Foreign Affairs of Japan, 'Basic Position of the Government of Japan on International Law Applicable to Cyber Operations', 28 May 2021, available at https://www.mofa.go.jp/policy/page3e_001114.html, at 5.

67 'Republic of Korea: Comments on the pre-draft of the OEWG Report', 14 April 2020, available at https://front.un-arm.org/wp-content/uploads/2020/04/200414-rok-comment-on-pre-draft-of-oewg.pdf ('Korea's Comments').

68 Council of the European Union, 'Declaration by the High Representative Josep Borrell, on behalf of the European Union, on malicious cyber activities exploiting the coronavirus pandemic', 20 April 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/.

recognised that due diligence obligations exist and apply to cyberspace.

In short, rules of general international law are not domain-specific, at least not by default. Instead, the starting point is that they apply across the board to different matters, contexts, areas, types of activity or domains, unless, and in so far as, their scope is implicitly or explicitly limited to one or more of these categories. Furthermore, rules or principles that lack such limitations and thereby of general applicability can be interpreted and applied to cover 'cyberspace'. When it comes to the concept of due diligence, neither of its iterations is limited to traditional physical domains, specific contexts or types of activity. In the same vein, its scope is sufficiently general to encompass cyber operations carried out by states and non-state actors, whether this assessment is framed as interpretation or identification. It is, of course, a different question whether the requirements of each primary rule of international law applicable to cyberspace are present in each given case, a question addressed in Chapter 4 below.

4. What is the meaning and function of a 'domain'?

As seen earlier, it is now common to treat cyberspace or ICTs as a new 'domain' of state activity. It is often assumed that, unlike the physical domains of air, land, sea, and outer space, cyberspace is an inherently different, *virtual* domain, where activities may take place without meaningful physical manifestations. But while belonging to one or another 'domain' is thought to be decisive as to the applicability of international law to a certain activity, the actual meaning and function of the concept have been largely overlooked.

In common parlance, 'domain' has a variety of meanings in different contexts. More traditionally, the word is associated with 'a territory over which dominion is exercised' or a 'region distinctively marked by some physical feature'.[69] But the meaning that international legal scholars seem to be referring to when they characterise 'cyberspace'

69 Merriam Webster, Definition of 'domain', available at https://www.merriam-webster.com/dictionary/domain. **t**

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

as a domain is that of a 'sphere of knowledge, influence, or activity',[70] 'a particular interest, activity, or type of knowledge'[71] or 'an area of interest or an area over which a person has control'.[72] Indeed, the so-called 'domains of public international law' seem to refer to the different branches of this legal system and their corresponding academic fields.[73] And these might cover one, more or all physical spaces, depending on the rule or set of rules in question. For example, international environmental law, a field of international law and academic study, applies to physical land, sea and airspace.

The idea that international law applies to or corresponds to different 'domains', whether these are areas of knowledge or physical spaces, seems to be derived from the context of armed conflict. There, the concept 'serves as a fundamental organizing idea, reflecting the way we conceptualize the battlefield and categorize actions taking place during armed conflict.'[74] Importantly, even in this context, the purpose of categorising a certain activity as falling within this or that domain, such as land, sea, air, or other types of battlefield or warfare, is not to exclude or carve out the given 'domain' from IHL's scope of applicability. In fact, 'much of IHL is not domain-specific and applies generally',[75] regardless of whether the act in question takes place in land, sea, air or any other space that matter, and irrespective of other specific features of the battlefield or act of warfare. To be sure, different, *different rules* of IHL or other fields of international law might apply to different aspects of the battlefield or acts of war, such as the protection of civilians and the regulation of means and methods of warfare. But the point is that IHL *as a whole* applies irrespective of whenever, wherever and however armed conflict takes place. Its 'domain' is only limited to armed conflict between states and/or

70 Ibid.

71 Cambridge Dictionary, Definition of 'domain', available at https://dictionary.cambridge.org/dictionary/english/domain.

72 Ibid.

73 Cornell Law School, Legal Information Institute definition of 'International Law', available at https://www.law.cornell.edu/wex/international_law.

74 Sarah McCosker, 'Domains of Warfare', in Ben Saul and Dapo Akande (eds.) *Oxford Guide to International Humanitarian Law* (Oxford University Press, 2020) 77, at 97

75 Ibid, at 78.

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

sufficiently organised armed groups. Which specific rule or principle applies to what particular situation is an entirely different matter, and does not negate their applicability, *in abstracto*, to the 'domain' of armed conflict.

As an 'organizing idea' that helps to conceptualise and/or classify different types of situations and the rules that cover them, the concept of 'domain' is inevitably artificial and subjective. Simply put, there is nothing inherent in international law or the situations that it covers that calls for their compartmentalisation into 'domains'. It is international lawyers and scholars who carve out those categories and classification on the basis of practical or scholarly considerations. Thus, for example, the choice to bundle up the rules of international human rights law into one category that covers certain state obligations vis-à-vis individuals arose as a result of the proliferation of human rights treaties after World War II.

In the same vein, the so-called 'physical' domains – land, air, sea, and outer space – are in part abstractions too. In reality, these 'areas' are seamlessly connected to form an organic whole. Yet in human understanding they have been separated or singled out for practical or scholarly purposes. The notions of 'territory' or 'space' more generally are themselves abstractions. They are nothing more than human projections of objects with a localised physical or imaginary existence. And as we shall see in the next section, just as physical domains have a 'virtual' dimension, so does 'cyberspace' have a variety of meaningful physical manifestations.

In sum, categorisations of places, events, objects or knowledge into 'domains', while helpful, should not be assumed to reflect or exhaust the scope of applicability of international law, especially when no such categorisation is implicit or explicit in the rule or principle in question.

5. Is cyberspace a 'domain' or 'space'?

The term 'cyberspace' features prominently in scholarly texts and official government pronouncements on how international rules and principles apply to 'cyber' operations perpetrated through ICTs. And it has now become a fertile 'domain' of legal, political and technical knowledge. But other than a shorthand for the accumulated knowledge on and interest in 'cyber' activities, is 'cyberspace' a space akin to the so-called land, air, sea and outer space 'domains'? In other words, whether or not one assumes that international law is domain-specific, what really is 'cyberspace' and to what extent does international law apply to it?

Understanding what 'cyberspace' is requires us to briefly go back to the origin of the term, its purpose and the background against which it was originally employed in legal discourse, before turning to its technical features. As other have noted, the prefix 'cyber' comes from the Greek word *kybernetes*, which means one who steers or governs, and alludes to the field of 'cybernetics' – defined as the study of remote control through devices[76] or 'command and control and communications in the animal [...] or the mechanical world'.[77] In contrast, the word 'space' not only has physical or geographical meanings but also philosophical, mathematical, social and psychological ones.[78] Quite telling but generally overlooked in the literature is the first use of the term in the 1960s to the designate the so-called 'as 'Atelier Cyberspace', an artistic partnership forged between architect Carsten Hoff and an artist Susanne Ussing.[79] Their work comprised a series of visual arts exhibitions containing sensory installations and images that depicted 'open systems', that is, architectural spaces adaptable to various influences, such as human movement and new material. According to Hoff himself:

76 Laurence Lessig, *Code: Version 2.0* (Basic Books, 2006), at 3.

77 Lior Tabanski, 'Basic Concepts in Cyber Warfare', 3 *Military and Strategic Affairs* (2011) 75, at 76, citing Norbert Wiener, Cybernetics or Control and Communication in the Animal and the Machine (The MIT Press & John Wiley and Sons, 1955).

78 Ibid, at 76.

79 Jacob Lillemose and Mathias Kryger, 'The (Re)invention of Cyberspace' (2015), *Kunstkritikk*, available at https://web.archive.org/web/20150826204717/http://www.kunstkritikk.com/kommentar/the-reinvention-of-cyberspace/.

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

> To us, "cyberspace" was simply about managing spaces. There was nothing esoteric about it. Nothing digital, either. It was just a tool. The space was concrete, physical.[80]

It was only in 1980s that the term started to be associated with computers and digital networks, following the publication of two works of science fiction by William Gibson – a short story entitled 'Burning Chrome'[81] and the novel 'Neuromancer'.[82] But not even Gibson himself assigned any technical meaning to the term. Instead, he defined it 'a consensual hallucination experienced daily by billions of legitimate operators, in every nation, [...] A graphic representation of data abstracted from the banks of every computer in the human system.'[83] Commenting on the more recent usage of 'cyberspace' to refer to the internet and other networks, Gibson confessed that:

> 'All I knew about the word "cyberspace" when I coined it, was that it seemed like an effective buzzword. It seemed evocative and essentially meaningless. It was suggestive of something, but had no real semantic meaning, even for me, as I saw it emerge on the page.[84]

Gibson's buzzword was subsequently taken up, quite effectively, in the early days of the internet by American political activists, such as John Perry Barlow, and legal theorists, among who were David Johnson and David Post.[85] As Julie Cohen notes, this is when the idea of 'cyberspace' *as a space* started to take shape.[86] Back then, labelling the internet and other networks as another space, different from the 'real world', was an attempt to treat it as a separate jurisdiction

80 Ibid.

81 William Gibson, *Burning Chrome* (Omni, 1982).

82 William Gibson, *Neuromancer* (Ace, 1984).

83 Ibid, at 69.

84 William Gibson *in* Mark Neale 'No Maps for These Territories' (Docurama, 2000).

85 See, for example, David R. Johnson and David Post, 'Law and Borders: The Rise of Law in Cyberspace', 48 *Stanford Law Review* (1996) 1379.

86 Julie E. Cohen, 'Cyberspace as/and Space', 107 *Columbia Law Review* (2007) 210, at 216.

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

to which state power, laws and regulations did not apply.[87] In line with the ultraliberal and utopian vision of the internet's pioneers, this virtual space – the new 'home of the Mind', as Barlow famously put it –[88] would instead be subject to the democratic will of its millions of users spread across the world.[89] In this light, it is not surprising that, more recently, we have seen states and international legal scholars referring to 'cyberspace' as a separate space or 'domain' for a similarly exclusionary purpose, i.e. to carve out 'cyberspace' from the scope of applicability of certain international rules or principles.

Nevertheless, even in American legal discourse, where the debate about internet governance and regulation was most fervent, the idea of an ungovernable or uncontrollable cyberspace was soon debunked. As early as 1996, in his controversial conference address, Frank Easterbrook immortalised the analogy according to which the law of 'cyberspace' was as real as the 'law of the horse'.[90] For him, there was neither need nor wisdom to conceive of new rules for the internet and other digital networks, as general rules continued to apply.[91] And in his comprehensive work on 'code as law', Lawrence Lessig explained how there is nothing inherently 'ungovernable' in the technical features or architecture of the Internet or 'cyberspace' for that matter.[92] As a human and thus political project and creation, 'cyberspace' can be perfectly designed to follow existing laws and used in a manner compliant with these, even if 'code' itself is a powerful tool to constrain human behaviour.[93] Though conceiving of 'cyberspace' as a virtual space, Lessig rightly observed that '[i]t will be regulated by real space regulation to the extent that it affects real space life, and it will quite

87 Ibid and Lessig, *Code 2.0*, *supra* note 76, at 288, 300-301.

88 Perry Barlow, 'Declaration of the Independence of Cyberspace', 8 February 1996, available at https://www.eff.org/cyberspace-independence.

89 Lessig, *Code 2.0*, *supra* note 76, at 2-3.; Cohen, *supra* note 86, at 216.

90 Frank H. Easterbrook, 'Cyberspace and the Law of the Horse', (1996) *University of Chicago Legal Forum* 207, at 208.

91 Ibid, at 2010.

92 Lessig, *Code 2.0*, *supra* note 76, at 3-6.

93 Ibid, 85-88.

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

dramatically affect real space life'.[94]

An important contribution to this debate was made by Jack Goldsmith,[95] Timothy Wu,[96] Dan L. Burk[97] and others who sought to demystify the nature of 'cyberspace'.[98] For them, the internet and other constituent parts of 'cyberspace' are simply 'communications networks', which are situated well within 'real space'.[99] In this sense, 'cyberspace' would be nothing but a metaphor to express simulated spaces or experiences, such as online gaming, dating or social media, or dating; or the 'virtual' prolongation or manifestation of real spaces, such as shops, public murals, government institutions or mailboxes, where the internet and other networks serve as tools for the performance or regular, 'real world' activities.[100] It is no more real than the worlds or places (re)created by books and films, or than the traditional paper or audio exchanges with friends, family or service providers, such as letters, receipts, or telephone calls. In the same vein, just like that global transportation networks do not give rise to a new 'world', or 'domain', so does cyberspace does not constitute a new 'space'.

This view is to a large extent true. In fact, looking at the more technical definition of the internet and other networks that are considered to be part of 'cyberspace' we see a range of digital technologies which enable us to communicate and process different types of data or information. And these technologies, such as computer applications, network links, and digital devices are themselves made up of complex

94 Laurence Lessig, 'The Zones of Cyberspace', 48 *Stanford Law Review* (1996) 1403, at 1406. See also Cohen, *supra* note 86, at 217-18.

95 Jack L. Goldsmith (1998) 'Against Cyberanarchy', 65 *University of Chicago Law Review* (1998) 1199; Jack Goldsmith, 'Regulation of the Internet: Three Persistent Fallacies', 73 *Chicago-Kent Law Review* (1998) 1119.

96 Timothy Wu, 'Application-Centered Internet Analysis', 85 *Virginia Law Review* (1999) 1163; Timothy Wu, 'When Law & the Internet First Met', 3 *Green Bag* (1999-2000) 171; Jack Goldsmith and Timothy Wu, *Who Controls the Internet?: Illusions of a Borderless World* (Oxford University Press, 2006).

97 Dan L. Burk, 'Legal Consequences of the Cyberspatial Metaphor', in Mia Consalvo et al. (eds) *Internet Research Annual Vol. 1: Selected Papers From the Association of Internet Researchers Conferences* 2000-2002 (2003) 17.

98 See Cohen, *supra* note 86, at 226-227.

99 Ibid.

100 Lessig, *Code 2.0*, *supra* note 76, at 9, 83.

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

layers of software, hardware and the data they process.[101] But as much as software and data – the 'virtual' or 'logic' layers of cyberspace – play a significant role in allowing one to control how these technologies operate, the input, processing and output of data through code depends on a physical substrate, just like human intelligence and reasoning depends on the human body and brain. Thus, hardware components such as cables, satellites, radio waves, computers and millions of silicon circuits, all located somewhere in the 'real world', are part and parcel of ICTs or 'cyberspace'.

Yet many lawyers, policy-makers and software programmers get so caught up in the potential of code in its virtual dimension, that they tend to forget that binary code itself, i.e., the 0s and 1s with which computer algorithms or languages are written[102] and which enable digital electronics to transmit data,[103] can only be processed by machines because of the logical way in which certain electric circuits– and perhaps DNA and quantum particles for the new generation of computers[104] – turn out to behave in nature.[105] These so-called 'logic circuits' are made up of 'logic gates' which yield an expected result when subjected to a certain voltage or signal.[106] It is by alternating these voltages in millions of circuits found in different hardware components, and by representing these voltages with logical and numeric values (i.e. 0s and 1s) that computer algorithms, that is, processing instructions such as '*if* x *then* do y', can be written in binary code.[107] In the same vein, we tend to forget that what allows

101 On the various layers of cyberspace, see Clare Sullivan, 'The 2014 Sony Hack and the Role of International Law', 8 Journal of *National Security Law and Policy* (2015) 437, at 454, fn 88.

102 Wikipedia contributors, 'Binary Code', available at https://en.wikipedia.org/wiki/Binary_code.

103 Wikipedia contributors, 'Digital electronics', available at https://en.wikipedia.org/wiki/Digital_electronics.

104 Darrel Ince, *The Computer: A Very Short Introduction* (Oxford University Press, 2011), at 122-126. See also IBM, 'What is quantum computing?', available at https://www.ibm.com/quantum-computing/learn/what-is-quantum-computing/; Martyn Amos, 'DNA computing', Britannica, available at https://www.britannica.com/technology/DNA-computing; Wikipedia contributors, 'Quantum computing', available at https://en.wikipedia.org/wiki/Quantum_computing; Wikipedia contributors, 'DNA computing', available at https://en.wikipedia.org/wiki/DNA_computing.

105 Wikipedia contributors, 'Electronic circuit', available at https://en.wikipedia.org/wiki/Electronic_circuit.

106 Wikipedia contributors, 'Logic gate', available at https://en.wikipedia.org/wiki/Logic_gate.

107 Wikipedia contributors, 'Boolean algebra', available at https://en.wikipedia.org/wiki/Boolean_algebra. See also Eyal Kushilevitz, 'Communication Complexity', in Marvin V. Zelkowitz, *Advances in Computers*, Volume 44 (Elsevier, 1997), available at https://www.sciencedirect.com/topics/computer-science/boolean-circuit.

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

software to create fascinating 'virtual machines' on our screens are the less-talked-about 'compilers', i.e. special programmes that translate high-level, sophisticated code into machine code that can be physically executed by a computer processor.[108] Therefore, even if advancements in computer power and programming languages have greatly improved connectivity and speed across national boundaries, and enhanced our perception of imaginary spaces such as 'The Cloud', the 'World Wide Web',[109] or virtual reality applications, these remain very much grounded in tangible physical infrastructure somewhere in the world.

However, it would also be too simplistic to stop there and reduce 'cyberspace', or ICTs, to their physical and logical layers. This is because perhaps the most important dimension or layer of what we call 'cyberspace' are the human beings and social structures that create, control and use ICTs, including their software, hardware and data. In this sense, 'cyberspace', or, more accurately, a multitude of cyberspaces, whether perceived differently or similarly to other spaces and technologies, is very much a human and social experience.[110] On the one hand, ICTs are shaped by 'real world' individual and collective activities, necessities and interests, such as government services, private communications, shopping, banking, leisure, etc. On the other hand, whether or not ICTs have any meaningful physical or kinetic manifestations in any object or place, they certainly affect the life of one or more individuals of flesh and bone located somewhere on Earth and beyond. As Lessig remarks, many people have been able to establish a true 'second life' online, with some playing games, expressing their own views or engaging in online social interactions, often more important than their offline social circles.[111] At the same time, what one does in cyberspace does not stay in cyberspace: the money one spends to play an online game goes to someone's pocket, the words one says publicly on the internet are potentially heard by its billions of users and

108 Tech Target Contributor, 'Complier' definition, available at https://whatis.techtarget.com/definition/compiler; https://www.britannica.com/technology/compiler.

109 The Science Museum, 'The World Wide Web: A Global Information Space', 14 November 2018, available at https://www.sciencemuseum.org.uk/objects-and-stories/world-wide-web-global-information-space.

110 Lessig, *Code 2.0*, *supra* note 76, at 84-85.

111 Lessig, *Code 2.0*, *supra* note 76, at 9, 12, 107-108.

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

every website one enters a trail of data is left and mined for commercial or political purposes by a variety of private or public entities.[112]

To give but one example of how changes in code and other ICT components may have a real-world impact,[113] take the recent 'SolarWinds' hack. This was a malicious cyber operation against a globally supplied network monitoring software which was carried out by inserting malicious code in the software's update and thereby enabled the hackers to breach the confidentiality of public and private data.[114] For this reason, the hack has been primarily framed as an information-gathering or cyberespionage operation, and one of a purely 'virtual' character.[115] Yet, even assuming that the hack was limited to a 'mere' digital data breach, this has already led to concrete financial losses and reputational damage to companies, government agencies and individuals around the world.[116] The costs of replacing the compromised systems are immense, and the public trust in the software, its providers and users is perhaps irreparably lost.[117] That cyber operation

112 Lessig, *Code 2.0*, *supra* note 76, at 20; Lessig, Zones, *supra* note 94, at 1406.

113 See UN GGE Report 2021, *supra* note 5, para 9 (finding that malicious use of ICT-enable covert information campaigns 'pose direct and indirect harm to individuals'); OEWG Final Substantive Report, *supra* note 4, paras 4 and 19 (noting the need to maintain a 'human-centric approach' to ICTs and that unlawful ICT activity 'could pose a threat not only to security but also to State sovereignty, as well as economic development and livelihoods, and ultimately the safety and wellbeing of individuals').

114 See, e.g., Kate O'Flaherty, 'SolarWinds: Microsoft Reveals New Details About Sophisticated Mega-Breach', *Forbes*, 16 February 2021, available at https://www.forbes.com/sites/kateoflahertyuk/2021/02/16/solarwinds-microsoft-reveals-new-details-about-sophisticated-mega-breach/; Kari Paul and Agencies, 'SolarWinds hack was work of "at least 1,000 engineers", tech executives tell Senate', *The Guardian*, 24 February 2021, available at https://www.theguardian.com/technology/2021/feb/23/solarwinds-hack-senate-hearing-microsoft; Christopher Bing, 'Suspected Russian hackers spied on U.S. Treasury emails – sources', *Reuters*, 13 December 2020, available at https://www.reuters.com/article/us-usa-cyber-treasury-exclsuive/suspected-russian-hackers-spied-on-u-s-treasury-emails-sources-idUKKBN28N0PG?edition-redirect=uk.

115 Jack Goldsmith, 'Quick Thoughts on the Russian Hack', *Lawfare*, 14 December 2020, available at https://www.lawfareblog.com/quick-thoughts-russia-hack; Kristen Eichensehr, '"Strategic Silence" and State-Sponsored Hacking: The US Gov't and SolarWinds', 18 December 2020, *Just Security*, available at https://www.justsecurity.org/73921/strategic-silence-and-state-sponsored-hacking-the-us-govt-and-solarwinds/; Asaf Lubin, 'SolarWinds as a Constitutive Moment: A New Agenda for the International Law of Intelligence', *Just Security*, 23 December 2020, available at https://www.justsecurity.org/73989/solarwinds-as-a-constitutive-moment-a-new-agenda-for-the-international-law-of-intelligence/; Ciaran Martin, 'Cyber "Deterrence": A Brexit Analogy', *Lawfare*, 15 January 2020, available at https://www.lawfareblog.com/cyber-deterrence-brexit-analogy.

116 Isabella Jibilian and Katie Canales, 'Here's a simple explanation of how the massive SolarWinds hack happened and why it's such a big deal', *Business Insider*, 25 February 2021, available at https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?r=US&IR=T; Kevin Poulsen, Robert McMillan and Dustin Volz, 'SolarWinds Hack Victims: From Tech Companies to a Hospital and University', *The Wall Street Journal*, 21 December 2020, available at https://www.wsj.com/articles/solarwinds-hack-victims-from-tech-companies-to-a-hospital-and-university-11608548402?page=1.

117 Edward Gately, 'Massive SolarWinds Hack Prompts Up to $25 Million in New Security Costs for Company', *Channel Futures*, 1 March 2021, available at https://www.channelfutures.com/security/massive-solarwinds-hack-prompts-up-to-25-million-in-new-security-costs-for-company; Gopal Ratnam, 'Cleaning up SolarWinds hack may cost as much as $100 billion', *Roll Call*, 11 January 2021, available at https://www.rollcall.com/2021/01/11/cleaning-up-solarwinds-hack-may-cost-as-much-as-100-billion/.

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

has also given the perpetrators remote control over certain critical infrastructure systems at least in the United States, such as power stations and distribution grids, which poses a very real risk of serious damage to critical public services, such as hospitals and schools.[118]

Thus, the term 'cyberspace', with its chiefly 'virtual' connotation, may be somewhat misleading, as it fails to capture the physical, human and social dimensions of ICTs. The term has also been used to purposefully sever these more tangible dimensions from the software and data layers, and in doing so, to exclude the latter from domestic and international regulation. For this reason, it is perhaps more accurate to refer to cyberspace not as a virtual or separate space, but as a set of multidimensional digital technologies – or ICTs – which are fully integrated with human activities that take place in different physical 'domains' or 'real life' spaces. As states themselves noted in the recent OEWG Final Substantive Report, 'the international security dimension of ICTs cuts across multiple domains and disciplines'.[119] After all, online resources and activities are not an end in themselves, but a means or tool to achieve different aims or effects that will usually manifest themselves, in different ways, in one or more of the traditional physical domains.

For present purposes, this means that those technologies remain fully subject to the rules and principles of international law, to the extent that they are relevant and applicable, and in so far as they have not been carved out by consistent state practice and *opinio juris*.[120] This includes the concept of due diligence, which, as we have seen, applies generally, by default, to all types of state activity – virtual, physical or social. Tellingly, that cyberspace is better framed as a set of digital technologies was already reflected in the language used in the various GGE reports, as well as the OEWG's mandate and documents, which

118 Joe Weiss and Bob Hunter, 'The SolarWinds Hack Can Directly Affect Control Systems', *Lawfare*, 22 January 2021, available at https://www.lawfareblog.com/solarwinds-hack-can-directly-affect-control-systems; Software Engineering Institute, CERT Coordination Center, 'SolarWinds Orion API authentication bypass allows remote command execution: Vulnerability Note VU#843464', *Carnegie Mellon University*, 26 December 2020, available at https://kb.cert.org/vuls/id/843464.

119 OEWG Final Substantive Report, *supra* note 4, para 10.

120 For a similar point, see Michael Schmitt, 'In Defense of Due Diligence in Cyberspace', 125 *The Yale Law Journal Forum* (2015) 68, at 73; Chircop, *supra* note 44, at 650.

refer precisely to 'information and communication technologies (ICTs)'. Similar framings, such as 'cyberspace' as a 'medium',[121] or 'the interdependent network of information technology infrastructures and resident data'[122], have been adopted by several states. Thus, when it comes 'cyber operations', it is more appropriate to frame questions of applicability of international law to new technological developments.

6. International law is technology-neutral

As has been noted elsewhere, the digital technologies that make up the internet and other information and communications networks are now far more advanced and complex than their older, analogue counterparts, such the telephone, radio, television, and even mobile telephony or earlier versions of the Internet. The speed, reach, pervasiveness, visibility and processing power of current ICTs are unprecedented. And in only a couple of years, when the number of components (or transistors) in an integrated circuit (or microchip) will have doubled, and the cost of computers halved,[123] many of the ICTs that we widely use today will have become outdated or even obsolete. For some, like Lawrence Lessig,[124] Julie Cohen,[125] and Jerry Kang,[126] this means that difference between the life we lead in 'real space', including through 'old' technologies, and the life we have forged through

121 See 'Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, Second Substantive Session – New York, 11 February 2020 Statement by the Delegation of Brazil, INTERNATIONAL LAW', 10-11 February 2020 ('Brazil's OEWG Statement') (referring to 'cyberspace' as a 'medium' of communications), available at http://webtv.un.org/search/4th-meeting-open-ended-working-group-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-second-substantive-session-10%E2%80%9314-february-2020/6131734500001/?term=%22Open%20Ended%20Working%20Group%22&lan=English&cat=Meetings%2FEvents&sort=date, timestamp 0:15:45.

122 US Department of Defense (DoD), 'Department of Defense Dictionary of Military and Associated Terms', Joint Publication 1-02 (8 November 2010, as amended through 15 March 2014), at 64; II.9.

123 Intel, 'Over 50 Years of Moore's Law', available at https://www.intel.co.uk/content/www/uk/en/silicon-innovations/moores-law-technology.html; Lee Bell, 'What is Moore's Law?', *WIRED* magazine (28th August 2016), available at https://www.wired.co.uk/article/wired-explains-moores-law; David Rotman, 'We're not prepared for the end of Moore's Law', *MIT Technology Review*, 24 February 2020, available at https://www.technologyreview.com/2020/02/24/905789/were-not-prepared-for-the-end-of-moores-law/; 'Moore's law', *Encyclopedia Britannica*, 26 December 2019, available at https://www.britannica.com/technology/Moores-law.

124 Lessig, *Code 2.0*, *supra* note 76, at 19, 26, 83-85.

125 Cohen, *supra* note 86, at 219-221.

126 Jerry Kang, 'Information Privacy in Cyberspace Transactions', 50 *Stanford Law Review* (1998) 1193, at 1198–1199.

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

'cyberspace' – or as we prefer to call it, ICTs – is not just one of degree but has unfolded or 'ripened' into one of kind.

This raises one fundamental question: Even if 'cyberspace' is not a separate space or domain, and international law applies in principle to all domains, are ICTs so different to other technologies that they cannot governed by existing international law? In other words, is there something *inherently different* about ICTs that carves them out from existing international law and, in particular, general international law? Alternatively, do technologies whose impact was unforeseen only a few decades ago, fall within the scope of traditional rules and principles of international law, such as sovereignty, the prohibition on the use of force, non-intervention and no-harm? Have these continued to stand the test of time? The answer to these and other similar questions seems to lie in a simple yet overlooked feature of international law, namely, that it is, by necessity, a technology-neutral system.[127]

Technological – or 'tech' – neutrality, in this sense, is not coterminous with political or economic neutrality in the 'tech world'. For the reality is that a few major corporations own or control a significant part of the internet's logical and physical infrastructure and provide the necessary software and hardware technologies that keep public and private online communications and information processing going. Thus, there is no neutrality when it comes to the economic and political forces that shape the use and distribution of ICTs around the world. But international law's 'tech neutrality' is something else: it refers to the fact that international rules and principles apply across the board to all technologies, old and new, at least by default and to the extent relevant.

To elaborate, 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, has never been enough reason to exclude them from the scope of application of existing rules

127 Second "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security, 27 May 2020, available at https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf ('Second OEWG Pre-draft'), para 21. See also Schmitt, *Tallinn Manual 2.0*, *supra* note 27, at 31, para 4 and at 46, para 12; *Responsibilities and obligations of States with respect to activities in the Area, Advisory Opinion*, 1 February 2011, International Tribunal for the Law of the Sea (ITLOS) Reports (2011) 10, para 117.

or principles, especially those of general application, such as tort, contract or criminal law. At the international level, the International Court of Justice recognised as much in its *Nuclear Weapons Advisory Opinion* when it held that:

> '39. These provisions [Articles 42 and 51 of the UN Charter] do not refer to specific weapons. They apply to *any* use of force, *regardless of the weapons employed*. The Charter neither expressly prohibits, nor permits, the use of *any specific weapon*, including nuclear weapons. [...]
>
> 85. [...] In the view of the vast majority of States as well as writers there can be no doubt as to the applicability of humanitarian law to nuclear weapons.
>
> 86. The Court shares that view. Indeed, nuclear weapons were *invented after most of the principles and rules of humanitarian law applicable in armed conflict had already come into existence*; the Conferences of 1949 and 1974-1977 left these weapons aside, *and there is a qualitative as well as quantitative difference between nuclear weapons and all conventional arms*. However, *it cannot be concluded from this that the established principles and rules of humanitarian law applicable in armed conflict did not apply to nuclear weapons*. Such a conclusion would be incompatible with the intrinsically humanitarian character of the legal principles in question which permeates the entire law of armed conflict and applies to *all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future*."[128]

Similarly, in its Draft articles on Prevention of Transboundary Harm from Hazardous Activities, the ILC noted that new technologies are also subject to *positive* duties to prevent transboundary harm, requiring states to employ scientific and technological developments to detect, prevent and redress harm, as well as ensure the safe use of those technologies:

128 *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*, 8 July 1996, ICJ Reports (1996) 226, paras 39 and 85-86 (emphasis added).

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

> (11) The standard of due diligence against which the conduct of the State of origin should be examined is that which is generally considered to be appropriate and proportional to the degree of risk of transboundary harm in the particular instance. [...] What would be considered a *reasonable standard of care or due diligence may change with time*; what might be considered an appropriate and reasonable procedure, standard or rule at one point in time *may not be considered as such at some point in the future*. Hence, due diligence in ensuring safety *requires a State to keep abreast of technological changes and scientific developments*.
>
> (14) Article 3 imposes on the State a duty to take all necessary measures to prevent significant transboundary harm or at any event to minimize the risk thereof. This could involve, inter alia, taking such measures as are appropriate by way of abundant caution, *even if full scientific certainty does not exist*, to avoid or prevent serious or irreversible damage. [....] An efficient implementation of the duty of prevention may well *require upgrading the input of technology in the activity as well as the allocation of adequate financial and manpower resources with necessary training for the management and monitoring of the activity*.[129]

Even more tellingly, the Chairs' Summary of discussions held at the UN OEWG, issued in May 2021 alongside the Group's Final Substantive Report, notes that:

> 'States emphasized that measures to promote responsible State behaviour *should remain technology-neutral, underscoring that it is the misuse of technologies, not the technologies themselves, that is of concern.*"[130]

129 International Law Commission (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, 2001, at 154-155, Commentary to Draft Article 3, paras 11 and 14 (emphasis added).

130 OEWG, Chair's Summary, UN Doc. A/AC.290/2021/CRP.3*, 10 March 2021, para 8 (emphasis added). See also very similar language in Second OEWG Pre-draft, supra note 127, para 21.

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

The OEWG is a multilateral and multi-stakeholder forum for discussion of pressing issues surrounding ICTs, including the applicability of international law to those technologies. Unlike the UN GGE on ICTs, whose membership is limited to a select group of 25 states, he OEWG is open to all UN member states, who can actively participate in the groups' oral discussions and the drafting of its documents. This means that its statements, including its findings on responsible state behaviour in cyberspace – whose framework includes both binding international law and non-binding norms – should not be taken lightly.

International law's '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. Accordingly, international legal rules or principles *of general applicability* – whether these are rules of customary international law, general principles or generally-framed treaty provisions – apply to *all technologies through* which states or non-state entities conduct their relevant activities. Importantly, this starting point means that there is no further need to prove their applicability to ICTs or other technologies via state practice and *opinio juris* that *specifically* refer to ICTs. These rules and principles, include, as we have seen earlier, the prohibition on the use of force, non-intervention, the Corfu Channel rule of 'due diligence', the no-harm principle, international human rights law and international humanitarian law. For their scope is sufficiently broad to cover ICTs, either via interpretation or deductive reasoning. It is the burden of those advocating for the exclusion of ICTs from the scope of these rules to present evidence to the contrary, i.e., that states, in their general practice accepted as law, have actively carved out ICTs from the scope of what are otherwise general rules and principles.

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.[131] These are necessary to account for certain specific features of digital technologies, such as their speed, connectivity, reach, pervasiveness and transboundary nature. That notwithstanding — and in line with the

131 Laurence Lessig, 'The Law of the Horse: What Cyberlaw Might Teach', 113 *Harvard Law Review* (1999) 501, at 503.

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

views expressed on the issue by an overwhelming majority of States — the starting point is the applicability of existing international law to *any* technology, rather than a legal vacuum.

To evoke, once again – and with a pinch of salt –, Frank Easterbrook's 'Cyberspace and the Law of the Horse', generality is not an enemy of good tech-governance.[132] Quite the opposite, as he notes, 'the best way to learn the law applicable to specialized endeavors is to study general rules.'[133] This is not to say that specific rules or regimes are unnecessary or irrelevant. As Lawrence Lessig observes, not only may ICTs' unique features benefit from specialised knowledge and regulation but may yield more general lessons about the nature and limits of the law as whole.[134] For instance, the power of code in defining the architecture of the internet is but one manifestation of how human behaviour and the law itself are constrained by natural or man-made 'architectures', such as mountains, rives, buildings, roads, and social structures.[135] At the same time, as man-made architectures, software and hardware are not static, and can very well be shaped and constrained by new and existing laws.

Nevertheless, the point is that specialised regimes for ICTs and other technologies cannot and should not displace more general rules of international and domestic law; these remain valid, applicable and inform the interpretation of more specific rules for 'cyberspace' and beyond. And there is a very good reason for that: in Easterbrook's words, we, lawyers and policy-makers 'don't know much about cyberspace; [and] what [we] do know will be outdated in five years (if not five months!)'.[136] In short, the applicability and flexibility of general rules and principles of international law are all the more important in the context of ICTs and new technologies, given their rapid development and complexity, which many of us cannot fully

132 Easterbrook, *supra* note 90, at 207-208.

133 Ibid, at 207.

134 Lessig, Horse, *supra* note 131, at 534-535.

135 Ibid, at 506-507.

136 Easterbrook, *supra* note 90, at 208.

grasp. New, specific and detailed treaty instruments would struggle to keep up to such speed, technical and scientific complexity. As a recent statement by the Czech Republic summarises, in guiding the applicability of international law to ICTs, a 'technology-neutral approach [...] provides a safeguard against rapidly evolving nature of ICT technologies.'[137]

7. Policy recommendations do not replace established international legal rules

As seen earlier, one objection to the applicability of certain international rules or principles of general applicability, such as those containing a standard of due diligence, is that, at times, these have been framed in normative or hortatory terms in official government statements. Two of these documents, and perhaps the most significant among them, are the 2013[138] and 2015[139] GGE consensus reports, which contain 'Recommendations on norms, rules and principles of responsible behaviour by States' in their use of ICTs. For instance, the 2013 GGE report makes the following recommendations for states, which seem to mirror existing rules or principles of international law, at least in part:

> 22. States *should* intensify cooperation against criminal or terrorist use of ICTs, harmonize legal approaches as appropriate and strengthen practical collaboration between respective law enforcement and prosecutorial agencies.
>
> 23. States must meet their international obligations regarding internationally wrongful acts attributable to them. States must not use proxies to commit internationally wrongful acts. States *should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs.*

137 Comments by the Czech Republic *supra* note 57, at 2.

138 UN GGE Report 2013, *supra* note 1.

139 UN GGE Report 2015, *supra* note 2.

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

> 24. States *should* encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs, including supply chain security for ICT products and services.
>
> 25. Member States *should* consider how best to cooperate in implementing *the above norms and principles of responsible behaviour*, including the role that may be played by private sector and civil society organizations. […][140]

More elaborately, the 2015 GGE report contains separate sections on 'How international law applies to the use of ICTs'[141] and 'Norms, rules and principles for the responsible behaviour of States'.[142] And in the latter section, we find an even longer list of recommendations. Like the 2013 GGE recommendations, they also seem to reflect a range of existing international rules and principles:

> (a) Consistent with the purposes of the United Nations, including to maintain international peace and security, States *should cooperate* 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; […]
>
> (c) States *should not knowingly allow their territory to be used for internationally wrongful acts using ICTs*;
>
> (d) States *should consider how best to cooperate* to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect;

140 UN GGE Report 2013, *supra* note 1 (emphasis added).

141 UN GGE Report 2015, *supra* note 2, paras 24-29, at 12-13.

142 UN GGE Report 2015, *supra* note 2, paras 9-15, at 7-8.

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

> (e) States, in ensuring the secure use of ICTs, *should* respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, *to guarantee full respect for human rights, including the right to freedom of expression*;
>
> (f) A State *should not conduct or knowingly support ICT activity contrary to its obligations under international law* that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;
>
> (g) States *should take appropriate measures to protect their critical infrastructure from ICT threats*, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions; […]
>
> (k) States *should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams* (sometimes known as computer emergency response teams or cybersecurity incident response teams) *of another State*. A State *should not* use authorized emergency response teams to engage in *malicious international activity*.[143]

The fact that both reports distinguish 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. To be sure, some of those norms do not reflect binding international law obligations. However, some of them do use, explicitly or implicitly, the language of law, and it is in those instances that questions arise as to legal status of the prescription in question.

143 Ibid, para 13 (emphasis added).

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

Arguments of this kind have been made about the concept of due diligence in cyberspace, which, as others have pointed out,[144] seems be encapsulated in paragraph 13(c) of the 2015[145] report and paragraph 26 of the 2013 report. Indeed, the language of these paragraphs is similar but not exactly identical to the principle articulated by the ICJ in its Corfu Channel case, which, as we shall see, refers to 'acts that affect the rights of other states, rather than 'internationally wrongful acts'.[146] But the fact that this provision has been phrased in normative terms ('should') and explicitly labelled as a 'non-binding, voluntary, norm of responsible state behaviour', as opposed to 'How international law applies to the use of ICTs'[147], has been taken by some to mean that the concept of due diligence is not binding or applicable in 'cyberspace'.[148] Furthermore, in both the 2013 and 2015 reports, states' duty not 'to use proxies to commit internationally wrongful acts using ICTs' appears alongside a recommendation that states 'should seek to ensure that their territory is not used by non-State actors to commit such acts'.[149] That many states have remained silent on the issue has only compounded the uncertainty around the applicability of due diligence in cyberspace.[150] Similar doubts might arise with respect to other rules that seem to be reflected in the voluntary, non-binding norms, such as duties to cooperate with other states in some circumstances, or the duty not to engage in or support activity contrary to international law, which seems to be subsumed within the broader rule of sovereignty.

144 Schmitt, Grey Zones, *supra* note 44, at 53-54. See also submission by Global Partners Regional *in* Australian Government, 'Public Consultation: responsible state behaviour in cyberspace in the context of international security - Summary of public submissions on developing best practice guidance on implementation of the 11 norms of responsible state behaviour in cyberspace articulated in the 2015 GGE Report (A/70/174), as endorsed by the UN General Assembly (A/RES/70/237)', June 2020, available at https://www.dfat.gov.au/sites/default/files/compilation-norm-implementation-guidance.pdf. ('Australia's Public Consultation'), at 4-5 ; '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', 29 May 2020 ('Australia's GGE Submission') (noting that [t]his norm is sometimes referred to as the "due diligence norm"), available at https://www.dfat.gov.au/sites/default/files/submission-by-australias-representative-to-the-gge-norm-implementation-may-2020.pdf; Korea's Comments, *supra* note 67.

145 UN GGE Report 2015, *supra* note 2.

146 See *Corfu Channel*, *supra* note 40, at 22.

147 UN GGE Report 2015, *supra* note 2, para 13(c) versus paras 24-28.

148 UN GGE Report 2015, *supra* note 2, at 7, para 10.

149 Ibid, para 28(e); UN GGE Report 2013, *supra* note 1, para 23.

150 Jensen and Watts, *supra* note 44, at 1573-1574; *Tallinn Manual 2.0*, *supra* note 27, at 31, Commentary to Rule 6, para 3 (acknowledging but rejecting this view); Australia's GGE Submission, *supra* note 144 (arguing that 'while there is no international consensus on whether due diligence is an international legal obligation applicable to State conduct in cyberspace, this norm has had universal endorsement (via A/Res/70/237)'); Submission by Institute for International Cyber Stability in Australian Public Consultation, *supra* note 144, at 5.

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

In this light, one may wonder whether certain well-established rules of international law have been reduced 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 above-mentioned statements issued by Argentina,[151] and, more recently, Israel,[152] New Zealand,[153] and the UK[154] which either deny or question the applicability of due diligence in cyberspace. In support of their view, those states contend that there is scant evidence of state practice and/or *opinio juris* in support of a 'cyber due diligence' rule.

However, this argument fails to observe that the articulation of these norms is without prejudice to states' rights and obligations under international law. This point has been eloquently raised by Finland in one of its intervention during the OEWG's 2020 session,[155] and Japan at the 2021 GGE meeting.[156] Indeed, paragraph 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 recent OEWG Final Substantive Report, adopted by consensus across all United Nations members:

> States reaffirmed that norms *do not replace or alter* States' obligations or rights under international law, which are binding, but rather provide *additional specific guidance* on what constitutes responsible

151 Argentina's Intervention at the 2nd Substantive GGE Meeting', *supra* note 14.

152 Schondorf, *supra* note 15.

153 New Zealand Ministry for Foreign Affairs and Trade, *supra* note 16.

154 UK Mission to the United Nations, *supra* note 11, para 12.

155 Finland, '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, February 10 and 11', February 2020, available at https://ccdcoe.org/uploads/2018/10/Statement-on-International-Law-by-Finnish-Ambassador-Janne-Taalas-at-2nd-session-of-OEWG.pdf, at 1-2.

156 Japan, Statement by Mr. AKAHORI Takeshi, Ambassador for United Nations Affairs and Cyber Policy of the Ministry of Foreign Affairs of Japan, on the adoption of the report by the Sixth GGE on Advancing responsible State behavior in cyberspace in the context of international security (Delivered in a closed online meeting of the GGE), 28 May 2021, available at https://www.un.emb-japan.go.jp/itpr_en/akahori052821.html (stating that 'while some of the 11 norms are related to international law, they do not alter any rights and obligations under international law. At the same time, lack of mention in this report does not mean that international rights and obligations not covered in the document are not applicable in cyberspace').

> State behaviour in the use of ICTs. Norms do not seek to limit or prohibit action that is otherwise consistent with international law.[157]

Similarly, one of the earlier versions of the OEWG substantive report recognises that:

> '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. [...] *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."[158]

and that:

> '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."[159]

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 paragraph 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. Likewise, it would make little sense if the recommendation contained in paragraph 13(k) of the 2015

157 OEWG Final Substantive Report, *supra* note 4, para 25. See also OEWG, 'Draft Substantive Report [Zero Draft], A/AC.290/[DATE], 19 January 2021 ('OEWG Zero Draft'), para 54.

158 Second OEWG Pre-draft, *supra* note 127, at page 7.

159 Ibid, para 38 (emphasis added).

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

GGE Report, calling upon states not to conduct or knowingly support activity other states' emergency response teams or engage in malicious international activity, were not reflective of an existing obligation under international law. And the recognition, in Norm 13(e), that States should 'guarantee full respect for human rights' online[160] would be hardly reconcilable with the inclusion of 'human rights and fundamental freedoms' as part of the international law applicable to States' use of ICTs.[161]

This conclusion is also in line with how several states have characterised the non-binding, voluntary norms of responsible state behaviour. First and foremost, the 2013 GGE Report explicitly notes that the norms are 'derived from existing international law relevant to the use of ICTs by States'.[162] In the same vein, the 2021 GGE Report recognizes that '[n]orms and existing international law sit alongside each other', and that '[n]orms do not seek to limit or prohibit action that is otherwise consistent with international law'.[163] France has also made it clear that these norms are an essential part of the framework of responsible state behaviour in cyberspace, and thereby are inseparable from the assessment of how binding international law applies in cyberspace.[164] Germany has also expressed the view that 'existing international law, complemented by the voluntary, non-binding norms that reflect consensus among States, is currently sufficient for addressing State use of ICTs'.[165] Japan has stated that 'international law and norms work together to prevent internationally wrongful acts using ICTs and to promote responsible State behavior in cyberspace'.[166] Along similar

160 UN GGE Report 2015, *supra* note 2, para 13(e); UN GGE Report 2021, *supra* note 5, paras 36-41.

161 UN GGE Report 2013, *supra* note 1, para 21; UN GGE Report 2015, *supra* note 2, para 26; UUN GGE Report 2021, *supra* note 5, para 70.

162 UN GGE Report 2013, *supra* note 1, para 16.

163 UN GGE Report 2021, *supra* note 5, para 15. See also UN GGE Report 2015, *supra* note 2, para 10.

164 France's Response, *supra* note 57.

165 Germany, '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', 6 April 2020 ('Germany's Comments on OEWG pre-draft'), available at https://front.un-arm.org/wp-content/uploads/2020/04/20200401-oewg-german-written-contribution-to-pre-draft-report-1.pdf.

166 Japan, *supra* note 156.

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

lines, states such as the UK,[167] France,[168] Poland,[169] Australia,[170] Brazil,[171] and the Dominican Republic,[172] as well as the International Committee of the Red Cross (ICRC)[173] have all affirmed that 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 may also be required as a matter of applicable international law. Where the norms do correspond to established rules of international law, the wealth of state practice and attitudes expressed in their implementation,[174] 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.

167 'Statement by UK Representative during UNSC Arria Formula Meeting on Cybersecurity', 22 May 2020, available at https://www.youtube.com/watch?v=K704P5D1n3E#action=share, timestamp 1:13:00; 'Press release: UK condemns cyber actors seeking to benefit from global coronavirus pandemic', 5 May 2020, available at https://www.gov.uk/government/news/uk-condemns-cyber-actors-seeking-to-benefit-from-global-coronavirus-pandemic; UK, 'Non-Paper on Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015', 1 September 2019, available at https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/uk-un-norms-non-paper-oewg-submission-final.pdf ('UK Non-Paper').

168 France's Response, *supra* note 57.

169 Poland, 'Statement by H.E. Tadeusz Chomicki Ambassador for Cyber & Tech Affairs Ministry of Foreign Affairs Arria-Formula Meeting of The Security Council on Cyber Stability, Conflict Prevention and Capacity Building', 22 May 2020, available at https://vm.ee/sites/default/files/Estonia_for_UN/statement_of_poland_arria_un_sc_on_cyber_22.05.2020.pdf.

170 '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)', 16 April 2020, available at https://front.un-arm.org/wp-content/uploads/2020/04/final-australia-comments-on-oewg-pre-draft-report-16-april.pdf.

171 'Statement by H.E. Mr. Ronaldo Costa Filho, Permanent Representative of Brazil to the United Nations During the Security Council Arria-Formula Meeting "Cyber Stability, Conflict Prevention and Capacity Building", 22 May 202, available at https://vm.ee/sites/default/files/Estonia_for_UN/statement_-_brazil_-_arria_formula_on_cybersecurity_-_final.pdf.

172 Dominican Republic's Statement, *supra* note 64.

173 ICRC, 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., available at https://www.icrc.org/en/document/norms-responsible-state-behavior-cyber-operations-should-build-international-law.

174 See UK Non-Paper, supra note 167; 'Canada's implementation of the 2015 GGE norms', 16 November 2019, available at https://www.un.org/disarmament/wp-content/uploads/2019/11/canada-implementation-2015-gge-norms-nov-16-en.pdf; 'Australian Implementation of Norms of Responsible State Behaviour In Cyberspace', 2020, available at https://www.dfat.gov.au/sites/default/files/how-australia-implements-the-ungge-norms.pdf.

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

When it comes specifically to due diligence, not only one but *several* norms of responsible state behaviour spelled out in the 2015 GGE report and further specified in the 2021 GGE report[175] recommend what are effectively different ways to comply with due diligence obligations in cyberspace.[176] This is particularly the case of the norms suggesting that states 'consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats';[177] 'take appropriate measures to protect their critical infrastructure from ICT threats'; 'respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts';[178] '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 'encourage 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'.[179]

Along with these recommendations to take *positive action*, norms that call upon states to *refrain* from harmful activities in cyberspace may also be necessary steps for states to comply with their international obligations to behave diligently when using ICTs. This includes the aforementioned recommendations 'not [to] conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public' and 'not [to] conduct or knowingly support activity to harm the information systems of the authorized emergency response teams

175 UN GGE Report 2021, *supra* note 5, paras 15-68.

176 For a similar view, see Comments by the Czech Republic, *supra* note 57.

177 UN GGE Report 2015, *supra* note 2, para 13(d).

178 On this norm, see remarks by the Institute for International Cyber Stability *in* Australia's Public Consultation, *supra* note144, at 12, linking this norm to the 'principle of due diligence', and arguing that the latter 'requires a State to take specific steps to mitigate any malicious ICT activity emanating from its territory' and remarks by the Tech Accord signatories that the principle of due diligence forms a key aspect of international law and that creates an additional duty to mitigate malicious ICT activity in this context.

179 Ibid, para 13(g), (h), (i) and (j).

The applicability of international law to information and communications technologies and the fallacy of 'cyberspace'

[...] of other States'.[180] In fact, as will become clearer in the course of this report, several intentional obligations containing a standard of due diligence, such as the no-harm principle and human rights obligations, not only require states to take positive action but also abstain from causing harm to individuals or other states.[181]

In sum, it seems that the voluntary, non-binding norms of responsible state behaviour in cyberspace, as well as similar policy recommendations are neither alternative to nor exhaustive of the binding obligations that they may allude to. On the contrary, norms or recommendations provide states with much welcome guidance on the interpretation, application and implementation of their existing international obligations in the ICT environment, particularly those containing a due diligence standard. This view is consistent with the flexible nature of such obligations, compliance with which can only be assessed on case-by-case basis, in light of all relevant factors and dynamic circumstances. This approach, unlike a specific 'domain-tailored' obligation, would 'up-date' itself to the constantly evolving technologies which is seeks to regulate, generating greater clarity in one's legal obligations.

In a nutshell, several norms of responsible state behaviour actually reflect and concretise existing due diligence obligations applicable in cyberspace. Although not binding per se and without prejudice to existing international law,[182] the norms are not deprived of any legal significance: they lay out possible, timely and widely accepted interpretations or understandings as to how existing due diligence obligations apply to ICTs.

180 Ibid, para 13(f) and (k).

181 See, e.g., ILC Draft Articles on Prevention *supra* note 129, at 159, Commentary to Article 8, para 2, and at 169, Commentary to Article 11, para 1; Human Rights Committee (HRC), '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, paras 25, 28-30; ECtHR (European Court of Human Rights), 'Guide on Article 2 of the European Convention on Human Rights: Right to Life', Updated on 31 December 2019, para 101.

182 See Finland, *supra* note 155.

8. Conclusion: The way ahead for cyber international law-making

General rules of international law apply by definition to all persons, objects, events and technologies that fall within their scope. Although some of these rules are limited to certain physical or natural spaces, such as air, land, sea and outer space, such limitations cannot be presumed, as international is not 'domain-specific'. And whether or not such limitations are found, they cannot, in and of themselves, exclude what we often call 'cyberspace'.

For one thing, the concept of 'domain' is not exclusionary, but fulfils a didactic function. For another, 'cyber' is not a space or domain, at least not like traditional physical space. Instead, it is a set of digital technologies, spread across multiple territorial boundaries and domains, which have been built by human beings to address different individual, social, political, cultural and economic needs. Even if their use has led to unique technical advances and human experiences, their impact remains very much grounded in the real world, ultimately affecting individuals and societies across the globe. Lastly, as domestic legal systems, international law does not discriminate on the basis of technology: it applies to each and every tool used by states or non-state actors in situations that fall under its extensive scope of application. As such, there is no question that international law applies to the Internet and other digital information and communications technologies – in their past, present and future iterations.

Granted, unlike history, international law can be re-written, provided that states agree to new rules by treaty or customary international law. However, the law that has been developed so far remains there, until such time as new rules will be developed. General rules and principles of international law continue to govern state behavior, irrespective of the technologies used. Should states decide to engage in a law-making effort, either aimed at one or more new treaties, or at the creation of new rules of customary international law through general practice

accepted as law, they must be aware that they are not building on a legal vacuum, but on the foundations of a wealth of existing binding rules. These rules have not only been affirmed but continue to be overwhelmingly applied and respected by the vast majority of states in the ICT environment, whether they expressly admit it or not.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

1. Introduction

As will be discussed in more detail throughout this report, though the nature and scope of 'due diligence' is contested, there is no question that the concept is, in essence, about *harm* prevention, mitigation and redress. And to the extent that it applies to states' use of ICTs, a preliminary factual question that arises is what types of 'cyber harm' the concept *may* cover. Put differently, against which factual background might states' exercise due diligence in their use of ICTs? We delve into specific harm thresholds under international law in Chapter 4. But before turning to legal concepts of harm and the standard of diligence that states must exercise in vis-à-vis ICTs, in this chapter, we set the scene with a discussion of the current landscape of 'cyber harms', i.e., the principal harms or risks that might materialise to or through ICTs. This landscape is characterised by an increased reliance on ICTs and other digital technologies for the exercise of public and private functions. Yet the widespread use of ICTs also leaves us more exposed to vulnerabilities which may cause accidental damage or can be exploited by malicious actors seeking to cause harm to different entities, objects or spaces.[1]

Unpacking the key aspects of this landscape will allow us to clarify key terms in the area, as well as to illustrate and shape the legal analysis that follows. To do that, we first identify the different ICT layers that might be targeted or otherwise suffer some kind of harm as a result of cyber activity, i.e., hardware, software, data and persons. Second, we classify the harms that one or more of those layers might suffer on the basis of on the quality or attribute affected: integrity, availability, confidentiality and content, for software, hardware and data, or tangible and non-tangible damage, for persons. Fourth, we apply this taxonomy in discussing common categories of cyber operations, such as distributed denial of service attacks, ransomware, spyware and remote access trojans. Lastly, we unpack the different actors – states,

1 See OEWG, Final Substantive Report, UN Doc A/AC.290/2021/CRP.2, 10 March 2021 ('OEWG Final Substantive Report'), paras 4, 15, 20-21; OEWG, Chair's Summary, UN Doc. A/AC.290/2021/CRP.3*, 10 March 2021, paras 7-8, 25. See also OEWG, 'Draft Substantive Report [Zero Draft], A/AC.290/[DATE], 19 January 2021, available at https://front.un-arm.org/wp-content/uploads/2021/01/OEWG-Zero-Draft-19-01-2021.pdf ('OEWG Zero Draft'), paras 4 and 17.

non-state groups and individuals – and relationships that might arise around these different cyberoperations.

2. Harm to different ICT layers

There is much talk and hype around the concepts of 'digital battlefield' and 'cyberwarfare', which in the US, for example, have fuelled prophecies and warnings about a possible 'cyber Pearl Harbor'.[2] This and other more visible threats, such as cyberattacks against hospitals, power plants and other critical infrastructure, have also led to speculation that a 'cyber Armageddon', 'digital doomsday' or 'cyber catastrophe' is likely.[3] These predictions are yet to materialise, and many cybersecurity and policy analysts are sceptical that they ever will.[4] In particular, a report commissioned by the Organisation for Economic Co-operation and Development concludes that few single cyber incidents have the capacity to lead to a 'global shock' – an event of a scale comparable to a pandemic, a natural disaster or an international financial crisis that has transboundary implications.[5] Though public and private entities are increasingly dependent on the Internet to carry out their daily activities, experts note that its decentralised and multi-layered architecture is such that it will be hard to hit all core networks, links and routers at once. Likewise, some believe that, as in the nuclear weapons context, the promise of mutually assured destruction through cyberweapons and cyber offensive capabilities will deter destructive cyber operations carried out by criminals and states.[6]

2 Adam Stone, 'How Leon Panetta's "Cyber Pearl Harbor" warning shaped Cyber Command', *Fifth Domain*, 30 July 2019, available at https://www.fifthdomain.com/opinion/2019/07/30/how-leon-panettas-cyber-pearl-harbor-warning-shaped-cyber-command/; Elisabeth Bumiller and Thom Shanker, 'Panetta Warns of Dire Threat of Cyberattack on U.S.', *The New York Times*, 11 October 2011, available at https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

3 Martin Courtney, 'Digital Doomsday', *Engineering & Technology Magazine*, 8 October 2019, available at https://eandt.theiet.org/content/articles/2019/10/digital-doomsday.

4 Ciaran Martin, 'Cyber Attacks: What actual harm do they do?', *RUSI*, 18 September 2020, available at https://rusi.org/event/cyber-attacks-%E2%80%93-what-actual-harm-do-they-cause, at 2-3.

5 Peter Sommer and Ian Brown, 'Reducing Systemic Cybersecurity Risk', *OECD/IFP Project on "Future Global Shocks"*, 14 January 2011, at 9-11, available at https://www.oecd.org/gov/risk/46889922.pdf, at 9-11.

6 See Sue Helpern, 'After the SolarWinds Hack, We Have No Idea What Cyber Dangers We Face, *The New Yorker*, 25 Jan 2021, available at https://

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

Yet the interconnectivity and interdependence across ICTs – public and private, military and civilian – mean that existing crises and catastrophes can either be magnified or mitigated by cyber activity.[7] This is precisely what has occurred in the context of the COVID-19 pandemic.[8] On the one hand, online services have alleviated the socio-economic impact of the health crisis. On the other, vulnerabilities in critical public services, such as hospitals, essential business and research activities, such as vaccine development and distribution, and individuals has been exploited by a range of cyber criminals, including nation-state actors.

In this section, we explore the locus of vulnerabilities which could lead to similar events, that is, the different ICT layers which may be directly targeted or collaterally affected by harmful cyber operations.

a. Harm to software

It is fairly common for malicious cyber operations to target or affect software. This is because by gaining access to and altering a software's so-called 'source code', whether by rewriting it or inserting new lines of code, perpetrators may be able to change the way in which a programme operates. As explained in Chapter 1, code or, more precisely, algorithms are the instructions or commands written in programming language that create and govern the operation of software. Malicious code, thus, is an umbrella term to describe code used to directly target, affect and cause harm to software which different actors, public and private, rely on. As we discuss in more detail in Section 4 below, the use of malicious code can take the form of a variety of well-known types of harmful operations, such as viruses, worms, Trojan horses, backdoors, malicious content and data leakage.[9]

www.newyorker.com/news/daily-comment/after-the-solarwinds-hack-we-have-no-idea-what-cyber-dangers-we-face; Mark Pomerleau, 'Are more robust cyber partnerships on the horizon?', *Fifth Domain*, 12 July 2019, available a https://www.fifthdomain.com/dod/2019/07/12/are-more-robust-cyber-partnerships-on-the-horizon/.

7 Sommer and Brown, *supra* note 5, at 12.

8 See OEWG Final Substantive Report, *supra* note 1, paras 4 and 26. See also OEWG Zero Draft, *supra* note 1, paras 4 and 55.

9 Veracode, 'Malicious Code', available at https://www.veracode.com/security/malicious-code.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

These codes can either be software themselves, i.e., auto-executable applications or malware, or simply web scripts designed to create system vulnerabilities and subsequently upload malware.[10] In essence, operations targeting software code may not only aim at the programme in and of itself but can be, and usually are, the entry point to affecting other ICT layers, such as data, hardware and, most importantly, individuals. This is especially true for pirated software, which are even more susceptible to malware.[11]

Crucially, software comprises not just the ordinary programmes that we run in our computers to generate text, images or calculations. It is everywhere on the Internet: from web browsers and networked applications, such as emails, search engines and social media platforms, to desktop programmes connected to Internet and the software that runs routers, servers and Internet of Things (IoT) devices, including self-driving vehicles, Amazon shopping, home and industrial appliances, such as sensors, thermostats and control valves in water treatment and energy distribution systems.[12]

In fact, software pervades all so-called 'layers' of the most used network model or protocol, namely TCP/IP, which stands for Transport Control Protocol and Internet Protocol. From the least to the most sophisticated, these layers are (see Figure 1): i) the Link layer, which connects computers, smartphones or other devices to the local area network (LAN) via wired (e.g. fibre optic cables) or wireless connection (radio waves or satellite); ii) the Internet or Internetwork layer, in charge of identifying and routing 'data packets' (i.e., fragments of information broken down into binary code) by assigning 'IP addresses' to different networks or devices and ensuring that sender's message arrives at its destination, regardless of the route taken ; iii) the Transport layer, which finds the best path to deliver data packets across network connections and routers around the world, whilst ensuring

10 Karspersky, 'What is Malicious Code', 02 February 2018, available at https://www.kaspersky.co.uk/resource-center/definitions/malicious-code.

11 Aaron Tan, 'Pirated software used to spread malware in APAC', *Computer Weekly*, 21 June 2017, available at https://www.computerweekly.com/news/450421136/Pirated-software-used-to-spread-malware-in-APAC.

12 Arm, 'What are IoT devices', available at https://www.arm.com/glossary/iot-devices; https://en.wikipedia.org/wiki/Internet_of_things; Wikipedia contributors, 'Internet of Things', available at https://en.wikipedia.org/w/index.php?title=Internet_of_things.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

the integrity of those packets; and iv) the Application layer, which, as the name suggests, corresponds to web applications that allow the end user to actually interact with and communicate through the Internet, including the World Wide Web (WWW) application and its browsers, mail applications and other networked applications which enable the sender (or 'client') to connect with its destination (i.e. the server) which may be located in any other network around the world.[13] All these different layers operate following a number of protocols, i.e., a set of rules or specification that define the way in which they communicate and function, which are then implemented through various programmes and in different ways using an appropriate programming language.[14]

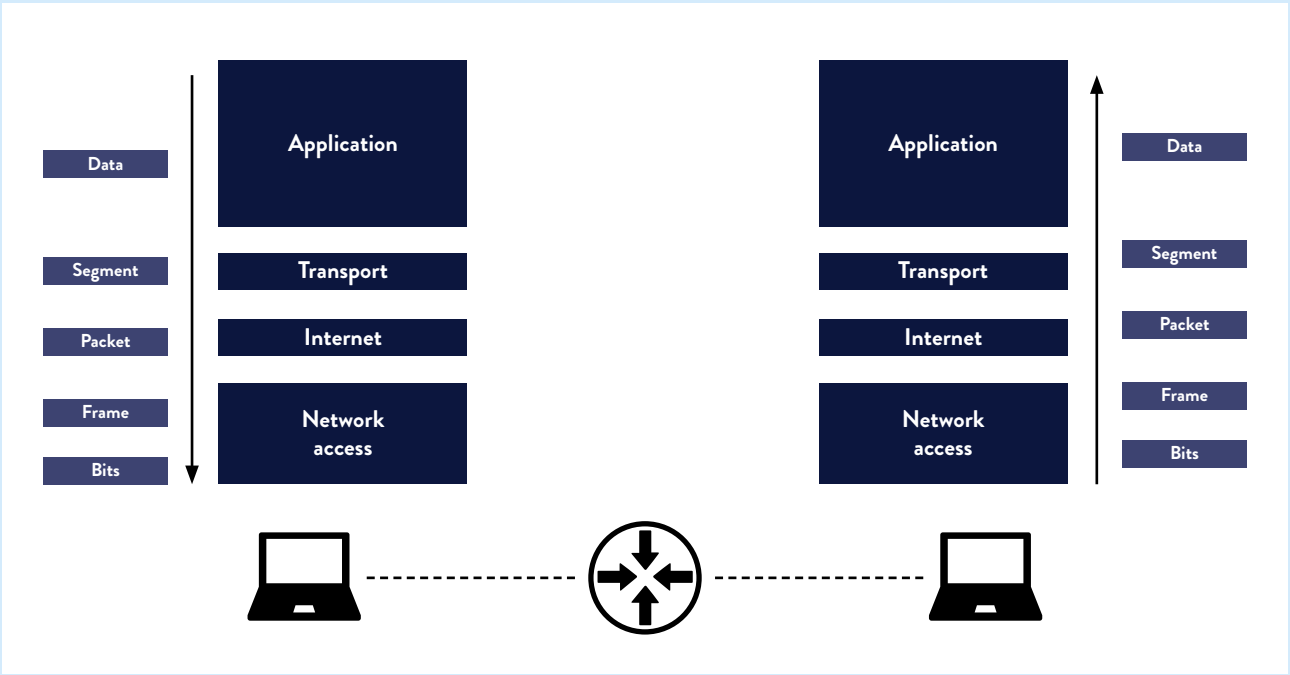

Figure 1: The TCP/IP Model of the Internet's layers.

Source: https://www.ccnablog.com/tcpip-and-the-osi-model/. Creative Commons Attribution License (reuse allowed)

13 Charles R. Severance, *Introduction to Networking: How the Internet Works* (Creative Commons, 2015), at 13-21.

14 Ibid, at 75, 83.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

For instance, the HyperText Transfer Protocol (HTTP) connects web clients to web services located through the Uniform Resource Locator (URL). It enables web browsers to retrieve websites on the Internet, containing text, images, audio or video, by using their IP addresses or web domains, which are assigned by another protocol called Domain Name System (DNS).[15] The HTTP protocol contains around 350 pages of rules and can be implemented in programmes such as web browsers, including Internet Explorer, Safari or Google Chrome, by using a variety of programming languages such as C, Python or Java.[16] Likewise, the Simple Network Management Protocol (SNMP) is a framework used for managing a variety of devices, i.e. physical objects, which are connected to the Internet but have limited or lacking user-interfaces.[17] Examples 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, home appliances and even medical equipment.[18] The SNMP protocol is implemented in network management or monitoring software, such as SolarWinds' Orion Network Performance Monitor, and Datadog's cloud-based system,[19] using programming languages such as Java.[20]

Given the pervasiveness of software on the Internet and other ICTs, a significant number of malicious cyber operations to date have targeted different networked applications.[21] Perhaps the most prominent among these are the 2007 'cyberattacks' on Estonia, attributed to Russian supports who protested the relocation of a Soviet-era statue

15 Ibid, at 75-77.

16 Ibid 76; It_qna contributor, 'In what- language- was-http- HTTP written- when- implemented-web on the Web', 15 January 2017, available at https://itqna.net/questions/494/what-language-was-http-written-when-implemented-web.

17 Nigel Lawrence and Patrick Traynor, 'Under New Management: Practical Attacks on SNMPv3', *WOOT'12: Proceedings of the 6th USENIX conference on Offensive Technologies*, August 2012, available at https://dl.acm.org/doi/10.5555/2372399.2372416, at 2.

18 Ibid.

19 Comparitech, '10 Best Network Monitoring Tools & Software of 2021, 21 January 2021, available at https://www.comparitech.com/net-admin/network-monitoring-tools/.

20 Oracle Corporation, 'Java Dynamic Management Kit 5.1 Tutorial, Chapter 17 Developing an SNMP Manager', available at https://docs.oracle.com/cd/E19698-01/816-7609/6mdjrf88m/index.html.

21 See 'Significant Cyber Incidents', *Centre for Strategic & International Studies*, available at https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

in Tallin.[22] The operation targeted a number of websites belonging to the government, the president, the parliament, police, banks, Internet service providers, online media, small businesses and local governments.[23] Different methods were used to overwhelm their web, e-mail and DNS servers as well as routers, such as the excessive sending of troubleshooting ('ping') messages, normally used to test connectivity using the Internet Control Message Protocol (ICMP), email spams, false web queries, website defacement and system hacking through insertion of malicious on different websites.[24]

Harms to software have become all the more prominent with the advent of brand-new applications whose uses, vulnerabilities and impact are only partly known. Examples include a) automated software feeding on Big data available on the Internet, such as search engines and text-generators using machine learning technology; b) Blockchain, also known as distributed ledger technology, which leads to decentralised decision-making in different applications, such as software developed for commercial transactions; and c) cloud computing, whereby data and computer power used for software are stored online by a third party.[25]

Yet, as the 2007 Estonia cyberattacks illustrate, malicious cyber operations targeting software often go beyond the 'logical' layer of cyberspace or ICTs to affect hardware, data or persons. In fact, software is often just a vehicle to harm other ICT layers, to which we now turn. Simply put, it is usually virus or parasitic code which either destroys or distorts the internal workings of the hardware which it attacks.

22 Rain Ottis, 'Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective', Cooperative Cyber Defence Centre of Excellence, 2008, available at https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf, at 1-2.

23 Ibid, at 2.

24 Ibid.

25 See Chair's Summary, *supra* note 1, para 8; OEWG Zero Draft, *supra* note 1, para 17.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

b. Harm to hardware

Computer 'hardware' refers to the physical parts of a computer and related devices.[26] This includes the central processing unit (CPU), the motherboard, computer storage, the computer case, its monitor, keyboard, mouse and the various circuits and wires that connect them together.[27] But in the age of smartphones, smartwatches and IoT, hardware goes well beyond mere computer parts to include a range of digital devices, many of which are connected to local networks or the Internet.[28] At their lowest level of abstraction, hardware components tend to follow the architecture developed by Jon von Neumann, which consists of five main parts: memory, the arithmetic logic unit, input devices, output devices, and the control unit.[29]

Cyber operations targeting or affecting hardware may occur in two principal ways. First, and less frequently these days, operations may directly target hardware by placing physical devices onto it, such as wiretaps, plugs, USB keys, or by physically manipulating hardware,[30] as is the case of introducing external or internal Trojans, i.e., changes to the circuitry of an integrated circuit,[31] manufacturing hardware backdoors for malware or other penetrative purposes,[32] signal interference or jamming,[33] overheating or power outages[34].

26 TechTerms, 'Harware Definition', available at https://techterms.com/definition/hardware.

27 Ibid and Wikipedia contributors, 'Computer Hardware', available at https://en.wikipedia.org/wiki/Computer_hardware.

28 TutorialsPoint, 'Internet of Things – Hardware', available at https://www.tutorialspoint.com/internet_of_things/internet_of_things_hardware.htm.

29 See Wikipedia contributors, 'Computer Hardware', *supra* note 27, and Jon von Neumann, 'First Draft of a Report on the EDVAC', University of Pennsylvania, 30 June 1045, available at https://web.archive.org/web/20130809184824/http://virtualtravelog.net.s115267.gridserver.com/wp/wp-content/media/2003-08-TheFirstDraft.pdf.

30 Eclypsium, 'Anatomy of a Firmware Attack', 19 December 2019, *Security Boulevard*, available at https://securityboulevard.com/2019/12/anatomy-of-a-firmware-attack/.

31 https://en.wikipedia.org/wiki/Hardware_Trojan Wikipedia contributors, 'Hardware Trojan', available at https://en.wikipedia.org/w/index.php?title=Hardware_Trojan&oldid=1009406424.

32 Pierluigi Paganini, 'Hardware attacks, backdoors and electronic component qualification', *INFOSEC*, 11 October 2013, available at https://resources.infosecinstitute.com/topic/hardware-attacks-backdoors-and-electronic-component-qualification/.

33 Weidong Fang, Fengrong Li, Yanzan Sun, Lianhai Shan, Shanji Chen, Chao Chen, Meiju Li, 'Information Security of PHY Layer in Wireless Networks', (2016) *Journal of Sensors*. 1-10, at 2.

34 European Union Agency for Network and Information Security (ENISA), Hardware Threat Landscape and Good Practice Guide, 8 February 2017,

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

An (in)famous example of such physical hardware operations came to light through the 'Edward Snowden revelations' in 2013: the United States (US) National Security Agency (NSA) requested a number of commercial technology companies to insert secret surveillance backdoors in their products, particularly mobile phones and laptops, so as to enable the NSA and other agencies, such as the UK's intelligence agency, the Government Communications Headquarters (GCHQ) to scan large amounts of traffic without a warrant.[35] These backdoors included USB cables with spy hardware and radio transceiver packed inside.[36] Similarly, the same revelations disclosed that GCHQ had installed over 200 taps or 'intercept probes' into transatlantic fibre optic cables crossing British shores.[37] This enabled the agency to collect vast amounts of telephone and online data, including recordings of phone calls, the content of email messages, Facebook entries, and users' browsing history, many of which were shared with the NSA and other members of the Five Eyes alliance, i.e., Canada, Australia and New Zealand.[38]

Second, cyber operations seeking to cause harm to hardware have increasingly used different types of software to reach a number of core computer components and other physical devices, as discussed in the previous section. In particular, many such operations consist of malicious code or physical devices targeting firmware, i.e. a less sophisticated type of software permanently embedded in hardware devices, such as a keyboards, hard drives, USB keys, cameras, printers and even remote controls.[39] Hardware and almost all electronic devices

available at https://www.enisa.europa.eu/publications/hardware-threat-landscape, at 16-18,. 23-24.

35 Joseph Mann, 'Spy agency ducks questions about 'back doors' in tech products', *Reuters*, 28 October 2020, available at https://www.reuters.com/article/us-usa-security-congress-insight-idUSKBN27D1CS; James Ball, Julian Borger and Glenn Greenwald, 'Revealed: how US and UK spy agencies defeat internet privacy and security', *The Guardian*, 6 September 2013, available at https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

36 Sean Gallangher, 'Your USB cable, the spy: Inside the NSA's catalog of surveillance magic', *ARS Technica*, 31 December 2013, available at https://arstechnica.com/information-technology/2013/12/inside-the-nsas-leaked-catalog-of-surveillance-magic/.

37 Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, 'GCHQ taps fibre-optic cables for secret access to world's communications', *The Guardian*, 21 June 2013, available at https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

38 Ibid.

39 ENISA, *supra* note 34, at 15-16 and 18; Kuntal Chakraborty, 'Firmware', *Techopedia*, 11 December 2016, available at https://www.techopedia.com/

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

depend on firmware to function, as it gives them basic instructions as to how to communicate with other devices and perform basic functions, such as input/output tasks.[40] Firmware attacks have been and can be used to insert malware into an operational system, collect data, remotely create a command-and-control channel to the infected device, and temporarily or permanently disable a device, such as a server.[41] An example of this type of operation are the so-called 'evil maid' attacks, whereby someone with physical access to a computer inserts a backdoor or rootkit device to, *inter alia*, exfiltrate or tamper with hard disk data, bypass security functionalities, and compromise computer hardware components.[42]

But unlike firmware attacks, other types of software can be used to compromise hardware devices without requiring someone to physically have access to a computer. This is notably the case of cyber operations against devices connected to the Internet via wired or wireless connection, such as IoT home and industrial appliances.[43] Worryingly, as noted earlier, to reduce costs and improve effectiveness, such devices are increasingly employed in critical services or infrastructure, such as water distribution systems, power plants, electrical grids, fuel processing facilities, telecommunications infrastructure, public transport, and the healthcare sector.[44] In the case of industrial processes, devices are usually remotely controlled via Industrial Control Systems (ICS), ranging from a few controllers to larger systems, such as supervisory control and data acquisition (SCADA) systems or distributed control systems (DCS), and programmable logic controllers

definition/2137/firmware#:~:text=Firmware%20is%20a%20software%20program,like%20basic%20input%2Foutput%20tasks.

40 Ibid and 'Firmware', Wikipedia, contributors, 'Firmware', available at https://en.wikipedia.org/wiki/Firmware.

41 Eclypsium, *supra* note 30.

42 ENISA, *supra* note 34, at 18; Micah Lee, 'It's Impossible To Prove Your Laptop Hasn't Been Hacked. I Spent Two Years Finding Out.', *The Intercept*, 28 April 2018, available at https://theintercept.com/2018/04/28/computer-malware-tampering/; Lorenzo Franceschi-Bicchierai, 'Watch a Hacker Install a Firmware Backdoor on a Laptop in Less Than 5 Minutes', *Vice*, 23 July 2018, available at https://www.vice.com/en/article/a3q374/hacker-bios-firmware-backdoor-evil-maid-attack-laptop-5-minutes.

43 See Chair's Summary, *supra* note 1, para 8; OEWG Zero Draft, *supra* note 1, para 17.

44 Courtney, *supra* note 3.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

(PLCs).[45] This means that their operation is vulnerable to infection by malicious code through the Internet and other networks, including those carried in email accounts, downloads, servers, and online databases.[46]

This is precisely what happened in the 2013 Stuxnet attack against Iranian nuclear centrifuges and the 2016 winter electricity blackouts in Ukraine. In the former, a computer worm first infected Microsoft Windows machines and networks over the Internet (or via USB sticks), replicating itself until it reached the Siemens Step7 SCADA software and the PLC systems which controlled Iran's high-speed nuclear enrichment centrifuges, at which point the worm exfiltrated information on industrial systems and caused one-fifth of centrifuges to tear apart.[47] In the latter, perpetrators orchestrated a spear-phishing campaign whereby malicious software hidden in an attached Microsoft word document was delivered to the email accounts of IT staff and system administrators of Ukrainian power distribution companies.[48] When downloaded, the malicious code infected machines and opened a backdoor which was subsequently used to map networks and credentials that employees used to remotely connect to power supply SCADA networks through Virtual Private Networks (VPN).[49] This enabled the perpetrators to reconfigure the backup power supply.[50] Malicious firmware was also installed on Ethernet energy converters to prevent workers from sending commands from the SCADA network to take a number of power substations off the grid.[51]

45 'Industrial control systems', Wikipedia contributors, 'Industrial control system', available at https://en.wikipedia.org/wiki/Industrial_control_system.

46 Courtney, *supra* note 3.

47 David Kushner, 'The Real Story of Stuxnet', *IEE Spectrum*, 23 February 2013, available at https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet; Wikipedia contributors, 'Stuxnet', available at https://en.wikipedia.org/wiki/Stuxnet.

48 Kim Zetter, 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid', *WIRED Magazine*, 3 March 2016, available at https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

49 Ibid.

50 Ibid.

51 Ibid.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

For some cybersecurity experts, ICS, other operational technology used to control devices, and geospatial information, rather than the IT networks and applications used to attack them, are the 'crown jewels' that states should be protecting.[52] Thus, whether or not 'Cyber Pearl Harbor' or 'digital Armageddon' are looming in our horizons, it is clear that cyber operations against hardware devices used for a number of essential or critical service have already caused serious harm and disruption, and risk wreaking further havoc. In this regard, states and IT companies should keep a close eye on the recent SolarWinds hack.[53] Whilst its most visible and talked-about aim appears to be the exfiltration of data belonging to IT companies and US governmental agencies, the perpetrators chose to target a network monitoring software which follows the SNMP protocol to exert operational control of a number of physical devices, including those found in US power grids and nuclear facilities.[54] Whether this software was purposively breached to gain control of critical devices remains to be see.

c. Data Harms

'Data harms', i.e., harms to or through data, are usually associated with the deletion or adulteration of digital information.[55] This is so for a number of reasons. First, there is little doubt that, if data is destroyed or altered, it may no longer hold its original value. Thus, as we discuss in Section 3 below, ransomware operations, such as Wannacry and NotPetya, have thrived on the threat of data deletion. Second, deletion or adulteration of data used by critical infrastructure, such as election ballot counting systems, or even the threat thereof, can be especially disrupting. For instance, allegations of Russian intrusion into voter-registration systems, state and local election databases, electronic poll

52 Courtney, *supra* note 3, citing *Accenture*, '2019 Cyber Threat Landscape Report', available at https://www.accenture.com/_acnmedia/PDF-107/Accenture-security-cyber.pdf, at 81.

53 On the concerns expressed by states about cyber operations against the integrity of ICT global supply chains, see Chair's Summary, *supra* note 1, paras 7, 25, 28 and pages 14, 17 and 19. See also OEWG Zero Draft, *supra* note 1, para 16.

54 Joe Weiss and Bob Hunter, 'The SolarWinds Hack Can Directly Affect Control Systems', *Lawfare*, 22 January 2021, available at https://www.lawfareblog.com/solarwinds-hack-can-directly-affect-control-systems.

55 See, e.g., 'Scenario 12: Cyber operations against computer data', *Cyber Law Toolkit*, available at https://cyberlaw.ccdcoe.org/wiki/Scenario_12:_Cyber_operations_against_computer_data.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

books and other equipment,[56] have led many to question the legitimacy of the 2016 US elections results.[57] Even though the US Cybersecurity and Infrastructure Security Agency (CISA) reassured the public that the 2020 elections had been the most secure in history,[58] allegations of foreign interference in voting systems[59] continue to generate disputes over the election results and sow significant division in the country.[60] Third, breaches of confidentiality or exfiltration of data which leave it untouched are often framed as 'mere cyber espionage', which, for a large majority of states and legal scholars, is permitted under international law. This has led many to assume that cyber espionage and other intelligence operations by digital means cause no harm to the data obtained. Yet the reality is that not only data exfiltration but also the production and/or publication of certain types of digital content may be damaging to the data itself and the public or private entities to whom it pertains.[61]

56 US Senate, 'Report of The Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in The 2016 U.S. Election, Volume 1: Russian Efforts Against Election Infrastructure With Additional Views', 10 January 2020, available at https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf. See also David E. Sanger and Catie Edmondson, 'Russia Targeted Election Systems in All 50 States, Report Finds', *The New York Times*, 25 July 2019, available at https://www.nytimes.com/2019/07/25/us/politics/russian-hacking-elections.html; The Tribune News Services, 'U.S. official: Hackers targeted voter registration systems of 20 states', *Chicago Tribune*, 30 September 2016, available at https://www.chicagotribune.com/nation-world/ct-hackers-target-election-systems-20160930-story.html.

57 Virginia Heffernan, 'Was the 2016 election legitimate? It's now definitely worth asking the question', *Los Angeles Times*, 28 July 2018, available at https://www.latimes.com/opinion/op-ed/la-oe-heffernan-trump-illegitimate-20180728-story.html; Dan Merica, 'Clinton opens door to questioning legitimacy of 2016 election, *CNN*, 19 September 2017, https://edition.cnn.com/2017/09/18/politics/hillary-clinton-russia-2016-election/index.html.

58 CISA, 'Joint Statement from Elections Infrastructure Government Coordinating Council & The Election Infrastructure Sector Coordinating Executive Committees', 12 November 2020, available at https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election.

59 Jane C. Timm, 'Fact check: Trump pushes baseless conspiracy about foreign interference in mail-in voting', *NBC News*, 22 June 2020, available at https://www.nbcnews.com/politics/donald-trump/ridiculous-claim-trump-pushes-baseless-conspiracy-about-foreign-interference-mail-n1231722; James Palmer, 'Why Trump Will Blame Beijing for a Biden Victory', *Foreign Policy*, 6 November 2020, available at https://foreignpolicy.com/2020/11/06/election-2020-trump-china-biden/; Gino Spocchia, 'Top cybersecurity official fired by Trump says allegations of foreign interference in 2020 election "farcical"', *The Independent*, 28 November 2020, available at https://www.independent.co.uk/news/world/americas/us-election-2020/chris-krebs-trump-campaign-fraud-conspiracy-cybersecurity-b1763176.html.

60 Blake Ellis and Melanie Hicken, 'They stormed the Capitol to overturn the results of an election they didn't vote in', *CNN*, 1 February 2021, available at https://edition.cnn.com/2021/02/01/us/capitol-rioters-non-voters-invs/index.html; Ed Pilkington, 'Donald Trump is gone but his big lie is a rallying call for rightwing extremists', *The Guardian*, 24 January 2021, https://www.theguardian.com/us-news/2021/jan/24/donald-trump-big-lie-american-democracy; Manu Raju and Jeremy Herb, 'House conservatives urge Trump not to concede and press for floor fight over election loss', *CNN*, 7 December 2020, available at https://edition.cnn.com/2020/12/07/politics/house-republicans-trump-biden/index.html; Anita Kumar and Gabby Orr, 'Inside Trump's pressure campaign to overturn the election', *Politico*, 21 December 2020, available at https://www.politico.com/news/2020/12/21/trump-pressure-campaign-overturn-election-449486.

61 See Joanna Redden, Jessica Brand and Vanesa Terzieva, 'Data Harm Record', *Data Justice Lab*, August 2020, available at https://datajusticelab.org/data-harm-record.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

In the case of sensitive or confidential information, the mere fact that data has been exposed to non-authorised users may signify a permanent loss of its value. To illustrate, attempts to 'steal' or breach the confidentiality of data relating to a number of COVID-19 vaccine candidates were widely reported in the media and in official documents.[62] If successful, those attempts could have tampered with clinical trial results and thus jeopardised the entire process of regulatory approval of the targeted vaccines, for which data confidentiality is key.[63] Indeed, leakage of information about which patients received placebos and vaccine doses could change the behaviour of trial participants in such a way that the trial results would no longer be reliable.[64] And according to cybersecurity experts, even the slightest intrusion in research databases may undermine the credibility of the entire dataset, since it is often difficult to identify the exact pieces of information that were accessed and the full extent of the data breach.[65] Also in the context of the COVID-19 pandemic, IBM uncovered a widespread cyber operation against the vaccine 'cold supply chain', i.e., different organisations in charge of ensuring the safe preservation of vaccines in temperature-controlled environments during their storage and transportation.[66] Through a spear-phishing campaign against organisation employees, the perpetrators used malicious code to gain access to sensitive information about vaccine

62 UK National Cyber Security Centre, 'Advisory: APT29 targets COVID-19 vaccine development', 16 July 2020, available at https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf; Dan Sabbagh, 'Hackers "try to steal Covid vaccine secrets in intellectual property war"', *The Guardian*, 22 November 2020, available at https://www.theguardian.com/world/2020/nov/22/hackers-try-to-steal-covid-vaccine-secrets-in-intellectual-property-war; Amy Walker 'UK "95% sure" Russian hackers tried to steal coronavirus vaccine research', *The Guardian*, 17 July 2020, available at https://www.theguardian.com/world/2020/jul/17/russian-hackers-steal-coronavirus-vaccine-uk-minister-cyber-attack; BioNTech, 'Statement Regarding Cyber Attack on European Medicines Agency', 9 December 2020, available at https://investors.biontech.de/news-releases/news-release-details/statement-regarding-cyber-attack-european-medicines-agency; 'Pfizer/BioNTech vaccine docs hacked from European Medicines Agency', *BBC News*, 9 December 2020, available at https://www.bbc.co.uk/news/technology-55249353.

63 Philip R. Krause, Thomas R. Fleming, Susan S. Ellenberg and Ana Maria Henao-Restrepo, on behalf of the World Health Organization's Ad Hoc Clinical Trial Expert Group, 'Maintaining confidentiality of emerging results in COVID-19 vaccine trials is essential', 2020 *Lancet* 396 (10263), 21-27 November 2020 1611–1613, available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7834563/. See also 'The Second Oxford Statement on International Law Protections of the Healthcare Sector During Covid-19: Safeguarding Vaccine Research', *Oxford Institute for Ethics Law and Armed Conflict*, 7 August 2020, available at https://elac.web.ox.ac.uk/article/the-second-oxford-statement.

64 Ibid.

65 Paula Fagan, 'How to detect a data breach', *IT Governance Blog*, 16 October 2018, available at https://www.itgovernance.co.uk/blog/how-to-detect-a-data-breach.

66 Claire Zaboeva and Melissa Frydrych, 'IBM Uncovers Global Phishing Campaign Targeting the COVID-19 Vaccine Cold Chain', *IBM*, 3 December 2020, available at https://securityintelligence.com/posts/ibm-uncovers-global-phishing-covid-19-vaccine-cold-chain/.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

distribution plans and processes.[67] Although the exact aim of the operations remains unclear, the fact that companies like Pfizer use IoT and GPS-enabled thermal sensors to monitor the location and temperature of vaccine shipments raises a red flag as to the risk of significant disruption and physical harm.[68]

Similarly, whether or not industrial espionage or intellectual property (IP) theft are lawful under international law, the value of the information stolen may never be restored. Antivirus company MacAfee estimates that cyber theft of industrial secrets costs companies around the world between 125–150 billion US dollars.[69] According to the European Commission, costs include lost business opportunities, negative impacts on innovation, increased cybersecurity expenses and reputational damage.[70] And though the financial costs of cyber espionage against the state are much harder to assess, exfiltration or disclosure of sensitive or confidential government information may cause harm well beyond the content layer of ICTs. To give but one example, the whistle-blower website WikiLeaks released secret government data on, *inter alia*, the identities of informants, human rights activists, journalists and dissidents, US diplomatic cables, documents and messages belonging to the US' Democratic National Committee.[71] According to then US State Department legal advisor, Harold Koh, the publication of those documents 'place(d) at risk the

67 Ibid. See also 'Coronavirus: Hackers targeted Covid vaccine supply "cold chain",' *BBC News*, 3 December 2020, available at https://www.bbc.co.uk/news/technology-55165552; Alex Hern and Dan Sabbagh, 'Cyberspies target Covid vaccine "cold chain" distribution network, *The Guardian*, 3 December 2020, available at https://www.theguardian.com/world/2020/dec/03/cyberspies-target-covid-vaccine-cold-chain-distribution-network; David E. Sanger and Sharon LaFraniere, 'Cyberattacks Discovered on Vaccine Distribution Operations', *The New York Times*, 3 December 2020, available at https://www.nytimes.com/2020/12/03/us/politics/vaccine-cyberattacks.html.

68 Kat Jercich, 'Vaccine distribution pipeline faces serious cybersecurity risks', *Healthcare IT News*, 099 December 2020, available at https://www.healthcareitnews.com/news/vaccine-distribution-pipeline-faces-serious-cybersecurity-risks; Deborah Adams Kaplan, 'Why cold chain tracking and IoT sensors are vital to the success of a COVID-19 vaccine', 11 August 2020, *Supply Chain Dive*, available at https://www.supplychaindive.com/news/coronavirus-vaccine-cold-chain-tracking-iot-sensor-technology/583168/.

69 Center for Strategic and International Studies (CSIS) and McAfee, 'Economic Impact of Cybercrime – No Slowing Down', 2018, available at https://www.mcafee.com/enterprise/en-gb/solutions/lp/economics-cybercrime.html.

70 European Commission, 'The scale and impact of industrial espionage and theft of trade secrets through cyber', *Publications Office of the EU*, 11 March 2019, available at https://op.europa.eu/en/publication-detail/-/publication/4eae21b2-4547-11e9-a8ed-01aa75ed71a1/language-en, at 27-28.

71 'Is Wikileaks putting people at risk?', *BBC News*, 23 August 2016, available at https://www.bbc.co.uk/news/technology-37165230; Katie Connolly, 'Has release of Wikileaks documents cost lives?, *BBC News*, 1 December 2010, available at https://www.bbc.co.uk/news/world-us-canada-11882092; Greg Myre, 'How Much Did WikiLeaks Damage U.S. National Security?', *NPR*, 12 April 2019, available at https://text.npr.org/712659290; Wikipedia contributors, 'List of material published by WikiLeaks', *Wikipedia*, available at https://en.wikipedia.org/wiki/List_of_material_published_by_WikiLeaks.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

lives of countless innocent individuals', 'on-going military operations, including operations to stop terrorists, traffickers in human beings and illicit arms, violent criminal enterprises and other actors that threaten global security', and 'on-going cooperation between countries'.[72]

Relatedly, with the advent of the World Wide Web and the explosion of social media platforms and messaging applications, the dissemination of false or misleading has had unprecedented impact beyond ICTs.[73] In particular, information operations designed to achieve political or strategic outcomes, such as disinformation campaigns, have not only undermined public confidence in online and offline content but also jeopardised the functioning of core public services.[74] Recent examples include the spread of false information about COVID-19, its treatments and vaccines, which lead a number of individuals to die or get seriously ill from drinking bleach or alcohol, and others to dismiss the seriousness of the virus or reject government approved vaccines.[75] Massive disinformation campaigns also occurred in the context of elections or other democratic processes in the US, the UK, Brazil and France.[76]

72 Harold Hongju Koh, 'State Department letter to Wikileaks', *Reuters*, 28 November 2010, available at https://www.reuters.com/article/us-wikileaks-usa-letter-idUSTRE6AR1E420101128.

73 See Samantha Bradshaw, Hannah Bailey and Philip N. Howard, 'Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation', *Oxford Internet Institute*, 13 January 2021, available at https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/127/2021/01/CyberTroop-Report20-FINALv.3.pdf.

74 Accenture, *supra* note 52, at 15-21.

75 Fabio Tagliabue, Luca Galassi and Pierpaolo Mariani, 'The "Pandemic" of Disinformation in COVID-19', 2020 *SN Compr Clin Med* 1-3, available at https://pubmed.ncbi.nlm.nih.gov/32838179/; Sahil Loomba, Alexandre de Figueiredo, Simon J. Piatek, Kristen de Graaf and Heidi J. Larson, 'Measuring the impact of COVID-19 vaccine misinformation on vaccination intent in the UK and USA', *Nature Human Behaviour* (2021), available at https://www.nature.com/articles/s41562-021-01056-1; Melinda Mills, 'COVID-19 vaccine deployment: Behaviour, ethics, misinformation and policy strategies', *The British Academy and The Royal Society*, 21 October 2020, available at https://royalsociety.org/-/media/policy/projects/set-c/set-c-vaccine-deployment.pdf; Talha Burki, 'The online anti-vaccine movement in the age of COVID-19', 10 *The Lancet* (2020), available at https://www.thelancet.com/journals/landig/article/PIIS2589-7500(20)30227-2/fulltext; Lois Backet, 'Misinformation "superspreaders": Covid vaccine falsehoods still thriving on Facebook and Instagram', *The Guardian*, 6 January 2021, available at https://www.theguardian.com/world/2021/jan/06/facebook-instagram-urged-fight-deluge-anti-covid-vaccine-falsehoods.

76 See, e.g., Julia Carrie Wong, '"Putin could only dream of it": how Trump became the biggest source of disinformation in 2020', *The Guardian*, 2 November 2020, available at https://www.theguardian.com/us-news/2020/nov/02/trump-us-election-disinformation-russia; Dan Sabbagh, Luke Harding, and Andrew Roth, 'Russia report reveals UK government failed to investigate Kremlin interference', *The Guardian*, 21 July 2020, available at https://www.theguardian.com/world/2020/jul/21/russia-report-reveals-uk-government-failed-to-address-kremlin-interference-scottish-referendum-brexit; Rachel Ellehuus and Donatienne Ruy, 'Did Russia Influence Brexit?', *Centre for Strategic and International Studies*, 21 July 2020, available at https://www.csis.org/blogs/brexit-bits-bobs-and-blogs/did-russia-influence-brexit; Augusto Saraiva, 'Tackling Disinformation in Brazil', *Foreign Policy*, 19 September 2020, available at https://foreignpolicy.com/2020/09/19/tackling-disinformation-in-brazil-interview-patricia-campos-mello/; Christopher Harden, 'Brazil Fell for Fake News: What to Do About It Now?', *Wilson Center*, 21 February 2019, available at https://www.wilsoncenter.org/blog-post/brazil-fell-for-fake-news-what-to-do-about-it-now; Jean-Baptiste Jeangène Vilmer, 'The "Macron Leaks" Operation: A Post-Mortem', *Atlantic*

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

In sum, computer data is the core of ICTs, and the sheer variety and frequency of data harms is a testament to its importance for different entities. Significantly, as the examples assessed above demonstrate, harms to or through data may produce wide-ranging effects beyond the technologies with which it is processed. This includes, in particular, economic, social, political, reputational and physical damage to states, non-state entities, such as corporations, and individuals.

d. Harm to Persons

This brings us to arguably the most significant yet overlooked targets of harmful cyber operations: persons, whether considered individually or collectively. The foregoing sections have shown how software, hardware and data can either be the target or the means of commission of such operations. However, behind (or ahead of) the physical, logical and content layers of ICTs are natural and legal persons. As argued in Chapter 1, cyber operations do not occur in a vacuum or virtual reality, but are part and parcel of, and have actual effects in the real world. Thus, whenever harm is caused to hardware, software or data, someone ultimately 'pays the price'.

As the examples of SolarWinds, Stuxnet and WikiLeaks illustrate, states and companies can suffer both tangible and non-tangible damage as a result of malicious cyber operations. At the very least, significant costs might be incurred to identify and patch ICT vulnerabilities, and to repair or replace the IT products affected. At worse, physical or digital assets, including software, hardware and data, may be lost, damaged or destroyed, and governmental or corporate activities may be seriously disrupted.[77] Cyber operations may also cause harm to the reputation of businesses and public confidence in governments.[78]

Council, June 2019, available at https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf; 'Fake news: Five French election stories debunked', *BBC News*, 15 March 2017, available at https://www.bbc.co.uk/news/world-europe-39265777.

77 Martin, *supra* note 4, at 4-5, 8-9.

78 Ibid., at 6-7.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

But while cyber harms to states and business justifiably raise serious concerns, legal and policy discourse around ICTs have paid little attention to their impact on individuals. As seen earlier, COVID-19-related operations, such as vaccine data breaches and disinformation campaigns, are a good example of how individuals' health may be indirectly affected by harms to software, hardware and/or data. Other times, however, individuals are the direct targets of malicious cyber operations. This can have significant implications on their private or professional lives as well as their reputation, freedom of expression, bodily integrity and even life.

For instance, spyware Pegasus was manufactured by Israeli company NSO to target specific individuals. Victims' mobile phones could get infected by multiple vectors, such as a single click on a malicious link sent by SMS or online applications, messages sent through Apple's iMessage or missed calls on WhatsApp, without the need for any user interaction.[79] Once installed, the malware subjects individuals to complete surveillance, i.e. it reads the user's messages and emails, listens to calls, captures screenshots and pressed keys, and exfiltrates browser history and contacts, even if the data is encrypted.[80] It was purchased and used by a number of states and non-state groups against journalists, human rights activists and defenders, lawyers, international investigators, political opposition groups, and other members of civil society.[81] Notably, there are allegations that Pegasus was used by Saudi Arabia to spy on journalist Jamal Khashoggi shortly before his murder and Jeff Bezos, Washington Post owner and Amazon's former CEO.[82]

79 Citizen Lab, 'NSO Group / Q Cyber Technologies: Over One Hundred New Abuse Cases', *Citizen Lab*, 29 October 2019, available at https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/; Bill Marczak, John Scott-Railton, Noura Al-Jizawi, Siena Anstis, and Ron Deibert, 'The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage "Zero-Click" Exploit', *Citizen Lab*, 20 December 2020, available at https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/.

80 John Snow, 'Pegasus: The ultimate spyware for iOS and Android', *Karspersky Daily*, 11 April 2017, available at https://www.kaspersky.com/blog/pegasus-spyware/14604/.

81 Catalin Cimpanu, '"Lawful intercept" Pegasus spyware found deployed in 45 countries', *ZD Net*, 18 September 2018, available at https://www.zdnet.com/article/lawful-intercept-pegasus-spyware-found-deployed-in-45-countries/. See also *supra* note 79.

82 Marczak and others, *supra* note 79; UN Office of the High Commissioner for Human Rights, 'UN experts call for investigation into allegations that Saudi Crown Prince involved in hacking of Jeff Bezos' phone', 22 January 2020, available at https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25488. See also Human Rights Council (HRC), 'Annex to the Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions: Investigation into the unlawful death of Mr. Jamal Khashoggi', UN Doc. A/HRC/41/CRP.1, 19 June 2019, paras 68-71; HRC, 'Mandate of the Special Rapporteur on extrajudicial, summary or arbitrary executions and mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: Annex One - Analysis of the Evidence of Surveillance of Mr. Bezos' personal phone,

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

The dissemination of sensitive or violent content may also have a direct impact on individuals. This is particularly the case of online hate speech, which is now commonplace on social media platforms.[83] The most shocking example of how it can be used to harm individuals occurred in the context of the Rohingya situation in Myanmar. There, dehumanizing and stigmatizing language against the Rohingya, both online and offline, was a key component of the state-backed campaign to ostracise the group,[84] which may have amounted to genocide, crimes against humanity and war crimes.[85] Since August 2017, when violence resurfaced in Myanmar's Rakhine state, over 9,000 Rohingya died in Myanmar, including 6,700 violent killings, and more than 700,000 Rohingya refugees have fled to Bangladesh.[86] As noted by the UN Independent International Fact-Finding Mission on Myanmar, '[t]he role of social media is significant. Facebook has been a useful instrument for those seeking to spread hate, in a context where, for most users, Facebook is the Internet.'[87]

As of October 2020, it is estimated that 4.66 billion individuals, i.e., 59% of the global population were active Internet users.[88] Of those,

Key Technical Elements', available at https://www.ohchr.org/Documents/Issues/Expression/SRsSumexFreedexAnnexes.pdf; Zach Whittaker, 'Dozens of journalists' iPhones hacked with NSO "zero-click' spyware", says Citizen Lab', *Tech Crunch*, 20 December 2020, available at https://techcrunch.com/2020/12/20/citizen-lab-iphone-nso-group/; Zach Whittaker, 'UN calls for investigation after Saudis linked to Bezos phone hack', *Tech Crunch*, 22 January 2020, available at https://techcrunch.com/2020/01/22/bezos-nso-group-hack/.

83 See 'Scenario 19: Hate speech', *Cyber Law Toolkit*, available at https://cyberlaw.ccdcoe.org/wiki/Scenario_19:_Hate_speech.

84 HRC, 'Report of the independent international fact-finding mission on Myanmar', Advance Edited Version, UN Doc. A/HRC/39/64, 12 September 2018, para 73. See also 'In Myanmar, "pervasive hate speech and shrinking freedom"', *Al Jazeera*, 5 March 2019, available at https://www.aljazeera.com/news/2019/3/5/in-myanmar-pervasive-hate-speech-and-shrinking-freedom.

85 HRC, *supra* note 84, paras 84-89. See also *Situation in the People's Republic of Bangladesh/Republic of the Union of Myanmar*, Decision Pursuant to Article 15 of the Rome Statute on the Authorisation of an Investigation into the Situation in the People's Republic of Bangladesh/Republic of the Union of Myanmar, ICC-01/19-27, 14 November 2019, ICC, Pre-Trial Chamber III, paras 63ff; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (The Gambia v. Myanmar)*, Provisional Measures Order, ICJ, 23 January 2020, paras 29-31, available at https://www.icj-cij.org/public/files/case-related/178/178-20200123-ORD-01-00-EN.pdf.

86 'MSF surveys estimate that at least 6,700 Rohingya were killed during the attacks in Myanmar', *Medecins Sans Frontieres*, 12 December 2017, available at https://www.msf.org/myanmarbangladesh-msf-surveys-estimate-least-6700-rohingya-were-killed-during-attacks-myanmar; 'Rohingya refugee crisis: Facts, FAQs, and how to help', *World Vision*, 12 June 2020, available at https://www.worldvision.org/refugees-news-stories/rohingya-refugees-bangladesh-facts.

87 HRC, *supra* note 84, para 74. See also Steve Stecklow, 'Why Facebook is losing the war on hate speech in Myanmar', *Reuters*, 15 August 2018, available at https://www.reuters.com/investigates/special-report/myanmar-facebook-hate/; Alexandra Stevenson, 'Facebook Admits It Was Used to Incite Violence in Myanmar', *The New York Times*, 6 November 2018, available at https://www.nytimes.com/2018/11/06/technology/myanmar-facebook.html.

88 Joseph Johnson, 'Global digital population as of October 2020', *Statista*, 27 January 2021, available at https://www.statista.com/statistics/617136/

3.96 billion, i.e., 51% of the world population, are social media users. The tendency is that these numbers keep rising.[89] This means that a significant proportion of civil society faces a daily risk of suffering a range of online harms, direct or indirect. And the seriousness of the harms seen so far is reason enough for greater emphasis to be placed on the human impact of cyber operations.

3. The Nature of Cyber Harms

Harms to different ICT layers may take numerous forms, and it is often the case that one single cyber operation causes different types of harm to software, hardware, data and/or people. Likewise, the same damage to one of those layers may have multiple aspects or implications. For instance, operations seeking to 'steal' data may occur by compromising hardware and/or infecting the target system with malicious software or code. And the data stolen may not only be accessed or obtained by the perpetrator(s) but also changed, deleted or rendered inaccessible for the victim. This may cause reputational, financial, psychological or physical harm to the victim(s). Given such variety and overlaps, it is arguably impossible to devise a comprehensive list of all cyber harms or to place them in watertight categories. Yet, for the purposes of this study, it is helpful to classify them on the basis of the attributes, properties, features or qualities of the ICT layer which have been affected in an operation.

a. Types of Harms to Software, Hardware and Data

For harms against software, hardware and data, the most widely used classification divides them into harms against the confidentiality, integrity and availability of the respective layer.[90] This classification is

digital-population-worldwide/.

89 Dave Chaffey, 'Global social media research summary August 2020', *Smart Insights*, 3 August 2020, available at https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/.

90 Yulia Cherdantseva and Jeremy Hilton, 'Information Security and Information Assurance: Discussion about the Meaning, Scope, and Goals', in Fernando Almeida and Irene Maria Portela (eds.), *Organizational, Legal, and Technological Dimensions of IS Administrator* (IGI Global Publishing, 2014), at 4.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

known as the CIA triad, with each attribute or property comprising one pillar of the triad.[91] It was originally devised[92] and has been extensively used in the field of information security (InfoSec), which aims at protecting the various stages or actions required during information processing, storage or transmission, by various means, including technical, organisational, human and legal.[93] Not surprisingly, the classification has featured in cybercrime treaties[94] as well as in legal and policy documents of an increasing number of states and intergovernmental organisations.[95] Given its simplicity, comprehensiveness and widespread use, this is the classification that we adopt in this study with respect to harms against software, hardware and data.

i. Confidentiality

Confidentiality, the first limb of the triad, refers to the protection of software, hardware or data from unauthorised access.[96] In other words, ICT logical, physical and content layers possess this attribute if they

91 Ibid and SmartEye Technology, 'Confidentiality, Integrity, & Availability: Basics of Information Security', available at https://smarteyetechnology.com/confidentiality-integrity-availability-basics-of-information-security/; Chad Perrin, 'The CIA Triad', *TechRepublic*, 30 June 2008, available at https://www.techrepublic.com/blog/it-security/the-cia-triad/; Commissum, 'The CIA Triad: The key to Improving Your Information Security', 12 October 2018, available at https://commissum.com/blog-articles/the-cia-triad-the-key-to-improving-your-information-security.

92 See Zella G. Ruthberg and Robert G. McKenzie (eds.), 'Audit and Evaluation of Computer Security', US Department of Commerce, National Bureau of Standards, Proceedings of the NBS Invitational Workshop held at Miami Beach, Florida, March 22-24', *NSB Special Publication* (1977) 500-19, at 214.

93 Cherdantseva and Hilton, *supra* note 90, at 10, 12-18, 37-38.

94 See Council of Europe, Convention on Cybercrime ('Budapest Convention') 2001 ETS 184, Preamble, para 9 and Title 1, Arts. 2-8; African Union Convention on Cyber Security and Personal Data Protection, adopted on 27 June 2014, Art. 25; Arab Convention on Combating Information Technology Offences, 21 December 2010, Arts. 6-11 and 14.

95 See, e.g., OEWG Final Substantive Report, *supra* note 1, paras 18, 26; OEWG Zero Draft, *supra* note 1, paras 21, 50 and 86; Brazil, 'National Information Security Policy', 26 December 2018, Art. 1, available at http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2018/Decreto/D9637.htm; Germany, 'Act on the Federal Office for Information Technology (BSI Act – BSIG)', 23 June 2017, available at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf?__blob=publicationFile&v=1, ss. 2(2), 8a and 8; South Africa, 'National Cybersecurity Policy Framework', 4 December 2015, available at https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf, Executive Summary, para 5; UK, 'Consent to Activities Related to the Security of NHS and Public Health Services Digital Systems (Coronavirus) Directions 2020', 24 April 2020, available at https://www.gov.uk/government/publications/security-of-nhs-and-public-health-services-digital-systems-coronavirus-directions-2020, s. 2; Philippines, 'Cybercrime Prevention Act of 2012, s. 2', available at https://lawphil.net/statutes/repacts/ra2012/ra_10175_2012.html, s. 2; 'Offences against the confidentiality, integrity and availability of computer data and systems', E4J University Module Series: Cybercrime, *UNODC*, available at https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/offences-against-the-confidentiality--integrity-and-availability-of-computer-data-and-systems.html.

96 Cherdantseva and Hilton, *supra* note 90, at 20; Commissum, *supra* note 91.

are free from intrusions or penetration by malicious or unauthorised system entities, such as code, software, physical backdoors or individuals. Although confidentiality ultimately seeks to protect the privacy of ICTs' end-users, the former is just one component of the latter.[97] The importance of confidentiality varies across layers, sectors and end-users, and there are different ways to secure it, as we discuss in Chapter 5.

Even minor breaches of confidentiality of data, software and hardware used for medical or scientific research can undermine public confidence therein, halting regulatory approval of research outputs and their use by the general population. Similarly, IP theft or industrial espionage, whereby the confidentiality of commercial models, formulas, and other ideals is breached, may lead to unfair market competition. Confidentiality is also essential in the public sector, where access to and/or leakage of classified or sensitive government information may, *inter alia*, compromise law enforcement or military operations, such as those relying on protected informants, and generally undermine public confidence in government, as WikiLeaks has demonstrated. Last, but by no means least, confidentiality of personal information, activity, communications and assets is a key element of individual privacy.

ii. Integrity

When it comes to software, hardware and data, having integrity means being complete, unmodified or sound.[98] In more detail, ensuring the integrity of software means that its source code, i.e., the algorithms that govern its functioning, remains intact or unchanged by unauthorised entities.[99] The integrity of hardware, on the other

97 Jason Andress, The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice (Syngress, 2014), at 240.

98 Cherdantseva and Hilton, *supra* note 90, at 7, 9 and 20; US, Committee on National Security Systems, 'National Information Assurance (IA) Glossary', CNSS Instruction No. 4009, 26 April 2010, available at https://www.dni.gov/files/NCSC/documents/nittf/CNSSI-4009_National_Information_Assurance.pdf, at 38.

99 Richard Bellairs, 'What Is Software Integrity? And How To Achieve It', *Perforce*, 5 June 2019, available at https://www.perforce.com/blog/qac/what-is-software-integrity.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

hand, pertains to the absence of physical or functional changes to its components that affect the way in which the device is supposed to operate.[100] Notably, IT supply chain vulnerabilities frequently affect 'system integrity', i.e. the integrity of a programme's code or a computer component, and there are a number of measures that can prevent or mitigate this type of harm.[101] Lastly, integrity in the context of data is the quality of being accurate and consistent over its lifecycle, or free from unauthorised modification.[102]

Harms to the integrity of data, software and hardware may have different implications, depending on the extent of the change, the end-user and the activity in question. For instance, the insertion of malicious code, software or firmware may not necessarily affect the functioning of a programme or hardware, even if system confidentiality is compromised. And some physical changes to hardware, such as the removal or insertion of peripherical computer components, such was cables or keyboards, might not necessarily alter the way in which the device or its applications operate. Similarly, minor changes to data may not necessarily compromise its integrity or value. Yet, in areas such as scientific research and healthcare, the slightest change in datasets, information, application or physical devices may cause significant and irreversible harm to the activity in question and its user.

iii. Availability

In the context of ICTs, availability is the quality of being accessible and useable upon demand by an authorised entity.[103] Although often overlooked, this quality is essential to the performance of any ICT-dependent activity. Indeed, if an ICT layer cannot be used or

100 See, e.g., US National Security Agency, Central Security Service, 'Validate Integrity of Hardware and Software', 22 June 2016, available at https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/validate-integrity-of-hardware-and-software.cfm.

101 See Stacy Simpson, 'Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain', *SAFECode*, 14 June 2010, available at https://safecode.org/publication/SAFECode_Software_Integrity_Controls0610.pdf. See also Chair Summary, *supra* note 1, paras 28 and pages 14, 17 and 19; OEWG Zero Draft, *supra* note 1, para 16.

102 Andress, *supra* note 97, at 6; Commissum, *supra* note 91; Chirs Brook, 'What is Data Integrity? Definition, Best Practices & More', *Data Insider*, 1 December 2020, available at https://digitalguardian.com/blog/what-data-integrity-data-protection-101.

103 Cherdantseva and Hilton, *supra* note 90, at 20; Andress, *supra* note 97, at 7; SmartEye Technology, *supra* note 91; Commissum, *supra* note 91.

accessed, be it data, software or hardware, it will hardly serve any purpose. But, again, the impact of harms to the availability of those layers will the depend on the extent of the malicious operation, its duration, as well as the importance of targeted asset and activity. For instance, if a non-essential government website is taken offline for a couple minutes, its users will not likely suffer any significant harm. Yet, if a power station is switched off even for a few minutes, through attacks against the availability of its software or devices, the harm caused may be significant. In the same vein, if redundant data is made unavailable during a ransomware attack, for example, it is unlikely that the victims will feel the need to pay the ransom. However, if the data targeted is unique and essential to the performance of the activity in question, such as patient data in the context of healthcare services, its unavailability will halt the provision of the services in question.

b. Types of Harms to Persons

As the foregoing discussion evinces, the impact of harms against the confidentiality, integrity or availability of software, hardware or data cannot be discussed in the abstract. Rather, its full extent can only be assessed and appreciated with reference to those who use and benefit from the logical, physical and content layers of ICTs, that is, persons. Yet assessing cyber harms to persons, whether individuals or collective entities, is necessarily a case-by-case endeavour, dependant as it is from factual circumstances, including objective and subjective factors. Thus, if it is hard to comprehensively list and classify harms to software, hardware or data, it is even harder to do the same for people. While this classificatory exercise is beyond the scope of this report, for present purposes, it suffices to raise two key points.

First, harms to software, hardware or data may affect people, including individuals, states or corporations, in tangible and intangible ways. Tangible cyber harms to people range from property destruction or interference to physical harms to the environment, human health, bodily integrity and even life. As mentioned earlier, breaches of confidentiality effected by WikiLeaks threatened the lives of specific

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

individuals, and COVID-19 disinformation campaigns have led, directly or indirectly, to significant loss of life. Similarly, a ransomware attack against Düsseldorf University Hospital in Germany during the pandemic was the first to directly result in the death of a patient, who did not resist the forced trip to another hospital after the cyber operation halted the life-saving treatment she was meant to receive.[104]

Conversely, non-tangible cyber harms to individuals include harms to privacy, mental health or well-being, education, free access to information or freedom of expression. The recent Blackbaud hack against the student database of a number of UK and US universities is a good illustration of how malicious cyber operations can have a significant impact on individual's privacy and education.[105] In the same vein, states, corporations and non-governmental organisations may suffer non-tangible harm to their finances and reputation as a result of cyber operations against their software, hardware or data. There is no better example of financial and reputational harm arising from a massive cyber operation than the SolarWinds hack, which caused the IT company significant loss of revenue and market value, reputational damage, material loss of customers, a slowdown in business performance and high remediation and legal costs, which, according to some analysist, will lead to a downgrading of the company's financial ratings.[106]

The second and perhaps the most important point worth making at this stage is that, whether or not harms to persons are tangible or intangible, there is no question that operations affecting the confidentiality, integrity or availability of software, hardware or data will somehow be felt by someone in 'the real world'. To reiterate, ICTs are not virtual creatures, but form a web which pervades all aspects

104 Catalin Cimpanu, 'First death reported following a ransomware attack on a German hospital', *ZDNet*, 18 September 2020, available at https://www.zdnet.com/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital; Joe Tidy, 'Police launch homicide inquiry after German hospital hack', *BBC News*, 18 September 2020, available at https://www.bbc.co.uk/news/technology-54204356; Melissa Eddy and Nicole Perlroth, 'Cyber Attack Suspected in German Woman's Death', *The New York Times*, 18 September 2020, available at https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html.

105 Joe Tidy and Leo Kelion, 'Blackbaud Hack: Universities lose data to ransomware attack', *BBC News*, 23 July 2020, available at https://www.bbc.co.uk/news/technology-53516413.

106 Kari Paul, 'SolarWinds: company at the core of the Orion hack falls under scrutiny', *The Guardian*, 16 December 2020, available at https://www.theguardian.com/technology/2020/dec/16/solarwinds-orion-hack-scrutiny-technology.

of human life, including the public, professional, personal, social and private spheres. The more individuals, states, corporations and other organisations depend on ICTs to perform their daily activities and functions, the blurrier line will be between harms to different ICT layers – logical, physical, content and personal. Two key implications follow on from this. On the one hand, it will be rare to encounter instances where cyber operations causing harm to software, hardware or data will not cause meaningful effects on persons, be those tangible or intangible. At the very least, cybersecurity costs will be incurred to identify the vulnerabilities and the extent of the harm, and, if necessary, to repair them. On the other hand, the distinction between tangible and non-tangible harms to persons is becoming increasingly difficult to draw and rank. Indeed, for an individual or a corporation, it may make no difference if it is their home or data that is destroyed or damaged. Thus, when discussing the various types of cyber harms throughout this report, we include tangible and non-tangible harms to persons and other ICT layers, unless specified.

4. A Typology of Harmful Cyber Operations

The growing exposure of individuals and institutions to the Internet, online resources and other networks has made it easier and less costly for malicious actors to devise and perpetrate cyber operations. Notably, it is estimated that there are currently 980 million types of malware, i.e., malicious software, and that 350,000 new pieces of malware are detected every day.[107] By the same token, the more interconnected we are, with the exponential expansion of the Internet of Things, the more vulnerable we become to such operations. In fact, there has been a steady increase in malicious cyberoperations, including a 600% uptick in cybercrime due to the COVID-19 pandemic.[108] Although the number of malware attacks and variants is declining overall, certain types of malicious cyberoperations are on

107 Bojan Jovanović, 'Malware statistics – You'd better get your computer vaccinated', *DataProt*, 22 November 2020, available at https://dataprot.net/statistics/malware-statistics/.

108 '2020 Cyber Security Statistics, The Ultimate List of Stats, Data & Trends,' *PurpleSec*, available at https://purplesec.us/resources/cyber-security-statistics/.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

the rise. This is particularly the case of IoT malware.[109] While painting a complete picture of the current cyber threat landscape is beyond the scope of this project, a glimpse of the main cyber operations affecting software, hardware, data and persons can help us understand the types of cyber harms that states must be protecting from under international law.

a. Denial of Service (DoS) Attacks

DoS attacks have been known since the 1980s but gained prominence when used during the 2007 Estonian cyberattacks.[110] They consist of cyber operations primarily affecting the availability of computer software, hardware and/or data, either by crashing or flooding systems with multiple unsolicited traffic requests.[111] They are still frequent today and can cause significant harm, especially when multiple compromised computer or device networks, often known as 'botnets', are used to perpetrate the attack, in which case they become Distributed Denial of Service (DDoS) Attacks.[112] Botnets are infected through malware, remotely controlled by the perpetrator(s) and then used to send an overwhelming number of connection requests which consume the victim's server bandwidth.[113] These can disrupt access to a number of Internet applications, such as websites, email systems, or online accounts.[114] With the proliferation of IoT devices, such as smartwatches and sensors, security vulnerabilities have increased and DDoS attacks have grown in magnitude.[115]

109 Sam Cook, 'Malware statistics and facts for 2021', *Comparitech*, 12 February 2021, available at https://www.comparitech.com/antivirus/malware-statistics-facts/https://www.comparitech.com/antivirus/malware-statistics-facts/.

110 Georgios Loukas and Gulay Öke, 'Protection against Denial of Service Attacks: A Survey', 0 (2009) *The Computer Journal* 1-19, at 1-2.

111 CISA, 'Security Tip (ST04-015): Understanding Denial-of-Service Attacks', 20 November 2019, available at https://us-cert.cisa.gov/ncas/tips/ST04-015..

112 Cloudflare, 'What is a DDoS attack?', available at https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack/

113 Ibid.

114 CISA, *supra* note 111.

115 Ibid.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

Among the victims of such operations are essential service providers, such as banks, e-commerce, media companies, or governmental agencies.[116] Though they do not typically result in data loss, they may take victims offline for long hours, resulting in financial and reputational losses. victim a great deal of time and money to handle.[117]

b. Ransomware

Ransomware is usually listed as 'the number one cyber threat', given its frequency, pervasiveness and impact.[118] It is a type of malicious software that encrypts the victim's data and demands a ransom payment to restore access thereto.[119] It can affect computer servers, desktops, laptops, tablets and smartphones, often spreading across networks to other devices.[120] If the ransom is not paid, the data or access thereto may be permanently lost. Multiple vectors can be used to target victims' systems, such as email attachments, phishing messages, or pop-out pages.[121] These types of attacks are on the rise as it becomes increasingly easy for perpetrators to obtain the necessary malware on the Dark Web. According to a 2020 European Union Agency for Cybersecurity (ENISA) report, 2019 saw a 365% increase in ransomware attacks against businesses when compared to 2018, which resulted in over €10 billion paid in ransoms.[122]

116 Palo Alto Networks, 'What is a denial of service attack (DoS)?', available at https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos.

117 Karsperky, 'Distributed Denial of Service: Anatomy and Impact of DDoS Attacks', 5 June 2018, available at https://usa.kaspersky.com/resource-center/preemptive-safety/how-does-ddos-attack-work; Rachel McCollin, 'DDoS Attacks Explained: Causes, Effects, and How to Protect Your Site', *Kinsta Blog*, 26 October 2020, available at https://kinsta.com/blog/what-is-a-ddos-attack/.

118 Jason Firch, '10 Cyber Security Trends You Can't Ignore In 2021', *Purplesec*, 31 December 2020, available at https://purplesec.us/cyber-security-trends-2021/#Ransomware.

119 Josh Fruhlinger, 'Ransomware explained: How it works and how to remove it', *CSO*, 19 June 200, available at https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html.

120 Acronis, 'How Can You Protect Yourself From Ransomware?', available at https://www.acronis.com/en-gb/articles/nhs-cyber-attack/.

121 Juliana De Groot, 'A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time', *Data Insider*, 1 December 2020, available at https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time.

122 ENISA, 'Threat Landscape 2020 – Ransomware', 20 October 2020, available at https://www.enisa.europa.eu/publications/ransomware, at 3.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

Worryingly, the same report found that 66% of healthcare organisation have experienced such types of malicious cyber operations in the same year.[123] Indeed, healthcare institutions are among the most vulnerable targets of ransomware, given their dependence on patient and medical data, the impact of their loss on human life and health, and the urgency to pay the ransom to recover them.[124] Thus, ransomware operations not only cause financial and reputational losses to businesses and government agencies, but may cause physical and psychological harm to individuals.

As mentioned earlier, the first death directly linked to a cyber operation was caused in 2020 by a ransomware attack on Düsseldorf University Hospital in Germany, during the COVID-19 pandemic. Back in 2017, the WannaCry ransomware targeted one-third (at least 80 out of the 236 trusts) of the UK's National Health Service (NHS) Trusts, as well as 603 primary care and other NHS organisations, including 595 GP practices.[125] This resulted in a 6% decrease in hospital admissions, including 1100 emergency patients, 3800 fewer in-patient emergency attendances, and 13,500 out-patient appointment cancellations.[126] Although none of the affected hospitals paid the ransom, the disruptions costed an estimated £5.9 million.[127] By exploiting a vulnerability on Microsoft Windows 7 operating system, the WannaCry ransomware affected 230,000 computers across 150 countries, many of which belonged to major public and private organisations such as Russia's Ministry of Interior, Spain-based Telefonica, America's FedEx, France's Renault, German railway company Deutsche Bahn, Chinese universities, and

123 Ibid.

124 Jan Lemintzer, 'Ransomware gangs are running riot – paying them off doesn't help', *The Conversation*, 17 February 2021, available at https://theconversation.com/ransomware-gangs-are-running-riot-paying-them-off-doesnt-help-155254; BDO, 'BDO's Fall 2019 Cyber Threat Report: Focus On Healthcare', October 2019, available at https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdos-fall-2019-cyber-threat-report-focus-on-health.

125 See Rory Cellan-Jones, 'Ransomware and the NHS -– the inquest begins', *BBC News*, 14 May 2017, available at https://www.bbc.co.uk/news/technology-39917278; Acronis, 'The NHS cyber attack', available at https://www.acronis.com/en-gb/articles/nhs-cyber-attack/.

126 S. Ghafur, S. Kristensen, K. Honeyford, G. Martin, A. Darzi & P. Aylin, 'A retrospective impact analysis of the WannaCry cyberattack on the NHS', 98 (2019) *npj Digital Medicine*, available at https://www.nature.com/articles/s41746-019-0161-6, at 4.

127 Ibid, at 2.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

Brazilian-Chilean Airlines LATAM.[128]

Similarly, later on in the same year, the ransomware known as 'NotPetya' targeted government institutions and corporations worldwide. Targets included Danish shipping company Maersk, all of whose business operations were affected, and Ukraine's main airport, state banks and even the Chernobyl nuclear power plant, whose automatic Windows-based sensors were shut down, forcing the site to monitor radiation levels manually.[129]

Cybersecurity experts predict that ransomware attacks will cost between USD 20 billion and 6 trillion annually by 2021.[130]

c. Spyware and other surveillance operations

Spyware is a broad term used to refer to malware that covertly exfiltrates the victim's data once installed in a computer, smartphone or another device.[131] It is one of the most common threats to Internet users, targeting especially individuals, alone or in bulk.[132] Spyware's capabilities range from monitoring one's Internet activity and tracking login credentials to accessing encrypted messages and calls.[133] The bulk of spyware activity is aimed at financial gain by obtaining

128 Acronis, *supra* note 128; Karspersy, 'What is WannaCry ransomware?', 8 June 2020, available at https://www.kaspersky.co.uk/resource-center/threats/ransomware-wannacry; 'Ransomware cyber-attack: Who has been hardest hit?', *BBC News*, 15 May 2017, available at https://www.bbc.co.uk/news/world-39919249.

129 Andy Greenberg, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, *WIRED Magazine*, 22 August 2018, available at https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/; '"NotPetya" cyber-attack hits international organisations', *Cyfor Blog*, available at https://cyfor.co.uk/notpetya-cyber-attack-hits-international-organisations/; Jacob Gronholt-Pedersen, 'Maersk says global IT breakdown caused by cyber attack', *Reuters*, 27 June 2017, available at https://www.reuters.com/article/us-cyber-attack-maersk-idUSKBN19I1NO.

130 Purplesec, *supra* note 108; Rob Sobers, '134 Cybersecurity Statistics and Trends for 2021', *Varonis: Inside Out Security Blog*, 1 February 2021, available at https://www.varonis.com/blog/cybersecurity-statistics/.

131 John P. Mello Jr., 'What is spyware? How it works and how to prevent it', *CSO*, 28 March 2019, available at https://www.csoonline.com/article/3384100/what-is-spyware-how-it-works-and-how-to-prevent-it.html *Software Lab*, 'What is Spyware? Top 5 Types & Examples', available at https://softwarelab.org/what-is-spyware/.

132 Alexander S. Gillis, 'Spyware', *TechTarget*, November 2019, available at https://searchsecurity.techtarget.com/definition/spyware.

133 Ibid.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

credit card numbers, banking information and passwords.[134] But, as seen earlier, many spyware and surveillance operations exploiting software or hardware vulnerabilities[135] have political aims, targeting certain classes of individuals, such as human rights activists, minority groups or journalists, as well as government entities or public figures.[136] Thus, although the direct impact of spyware is the breach of data confidentiality, such operations may cause economic, reputational, phycological and even physical harm to individuals whose information may be extracted used for malicious purposes.

We tend to associate bulk or targeted electronic surveillance operations with sophisticated malware and devices,[137] such as the ones employed in the surveillance programmes of the US' NSA[138] and Central Intelligence Agency,[139] the UK's GCHQ[140] and the Russian System for Operative Investigative Activities.[141] More recently, concerns were raised about government misuse of different mobile surveillance methods, including stealthy Pegasus spyware,[142] developed by the Israeli company NSO,[143] British-manufactured fake cell towers which

134 Ibid.

135 On hardware-based spyware see Matt Day, Giles Turner, and Natalia Drozdiak, 'Amazon Workers Are Listening to What You Tell Alexa', *Bloomberg*, 10 April 2019, available at https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio.

136 See Stephanie Kirchgaessner and Jennifer Rankin, 'WhatsApp spyware attack: senior clergymen in Togo among activists targeted', *The Guardian*, 3 August 2020, available at https://www.theguardian.com/technology/2020/aug/03/senior-clergymen-among-activists-targeted-by-spyware; Nick Hopkins and Dan Sabbagh, 'WhatsApp spyware attack was attempt to hack human rights data, says lawyer', *The Guardian*, 14 May 2019, available at https://www.theguardian.com/technology/2019/may/14/whatsapp-spyware-vulnerability-targeted-lawyer-says-attempt-was-desperate; Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert, 'Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries', *The Citizen Lab*, 18 September 2018, available at https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

137 See generally HRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', UN Doc. A/HRC/41/35, 28 May 2019, paras 7-14.

138 See *supra* notes 35 and 36, and 'Wikipedia, contributors, 'PRISM (surveillance program)', available at https://en.wikipedia.org/wiki/PRISM_(surveillance_program).

139 See WikiLeaks, 'Vault 7: CIA Hacking Tools Revealed', 7 March 2017, available at https://wikileaks.org/ciav7p1/.

140 See *supra* note 35 and Wikipedia contributors, 'Tempora', available at https://en.wikipedia.org/wiki/Tempora.

141 Zach Whittaker, 'Documents reveal how Russia taps phone companies for surveillance', *TechCrunch*, 18 September 2019, available at https://techcrunch.com/2019/09/18/russia-sorm-nokia-surveillance/; James Andrew Lewis, 'Reference Note on Russian Communications Surveillance', *CSIS*, 18 April 2014, available at https://www.csis.org/analysis/reference-note-russian-communications-surveillance.

142 Wikipedia contributors, 'Pegasus (spyware)', available at https://en.wikipedia.org/wiki/Pegasus_(spyware).

143 See *supra* notes 79, 80, 81 and 82.

intercept mobile calls, known as International Mobile Subscriber Identity catchers or Stingray,[144] and Deep Packet Inspection devices, which monitor, analyse and redirect Internet and other network traffic.[145] Nevertheless, there is a wide range of simpler spyware and electronic surveillance techniques spread across the internet which tend to receive far less attention from states and the media. Examples include: a) adware, which is often built into free software or websites to monitor the user's online activity and display targeted ads, whose most prominent iteration are website cookies, which track and record users' personally identifiable information and Internet browsing habits; and b) keyboard loggers, which tracks users' physical or digital keystrokes usually to steal credentials or other personal information;[146] and c) facial and affect recognition software, which has been used by some states to target minority groups, such as the Uighurs in China.[147]

d. Remote Access Trojan (RAT) or Backdoors

Remote Access Trojan (RAT) is a type of malware that allows the perpetrator(s) to gain unauthorised access into the victim's computer or device and remotely control it undetected. This access is known as a 'backdoor'.[148] Once opened, the backdoor allows for a wide array of malicious operations, including breaches of data confidentiality or integrity, such as the monitoring of user behaviour or file deletion, as well as harms to software and hardware integrity, availability

144 Sofia Tomacruz, 'You think your data, communication devices are safe? Think again', *Rappler*, 17 March 2018, available at https://www.rappler.com/newsbreak/iq/philippines-government-surveillance-equipment-software.

145 Bill Marczak, Jakub Dalek, Sarah McKune, Adam Senft, John Scott-Railton, and Ron Deibert, 'BAD TRAFFIC: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?', *Citizen Lab*, 9 March 2018, available at https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/; Duncan Geree, 'How deep packet inspection works', *WIRED Magazine*, 27 April 2012, available at https://www.wired.co.uk/article/how-deep-packet-inspection-works.

146 Mello Jr. and Software Lab, *supra* note 131; Gillis, *supra* note 132.

147 Paul Mozur, 'One month, 500,000 face scans: how China is using A.I. to profile a minority', *The New York Times*, 14 April 2019, available at https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html; Paul Mozur and Don Clark, 'China's Surveillance State Sucks Up Data. U.S. Tech Is Key to Sorting It', *The New York Times*, 20 Jan 2021, available at https://www.nytimes.com/2020/11/22/technology/china-intel-nvidia-xinjiang.html.

148 Andrada Fiscutean, 'From pranks to APTs: How remote access Trojans became a major security threat', *CSO*, 9 November 2020, available at https://www.csoonline.com/article/3588156/from-pranks-to-apts-how-remote-access-trojans-became-a-major-security-threat.html; Malware Bytes Lab, 'Remote Access Trojan (RAT)', 9 June 2016, available at https://blog.malwarebytes.com/threats/remote-access-trojan-rat/.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

and confidentiality, such as permanent changes to source codes or destruction of hardware devices.[149]

This type of malware can be installed through several vectors, such as email attachments, web links or download packages, which are often blended with social engineering tactics or temporary physical access to the victim's computer or device. RATs have increased in number, variety and scope with the proliferation of IoT devices, which can be used either as vectors or targets of such backdoors.[150] Recent examples of RAT attacks include the SolarWinds hack, where software vulnerabilities allowed backdoors with remote access to be spread across software users,[151] the attack on the Ukrainian power grid in 2015, which used the 'BlackEnergy' malware to take control of power grid operators,[152] the hacking of Hillary Clinton's 2016 presidential election campaign,[153] and of the email accounts of Bellingcat's open-source researchers investigating the missile strike on MH17 and the Skripal poisonings.[154]

e. Computer Viruses and Worms

A computer virus is a type of malware that is inadvertently triggered or activated by the victim, to self-replicate and propagate into the operational system that it has infected.[155] Viruses can corrupt or

149 EUROPOL, 'How to protect yourself against remote access trojans and other malware', available at https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/how-to-protect-yourself-against-remote-access-trojans-and-other-malware.

150 Cameron Abbott, 'Interlopers in Things? IOT Devices May be used as Backdoors to your Network', *The National Law Review*, 27 August 2019, available at https://www.natlawreview.com/article/interlopers-things-iot-devices-may-be-used-backdoors-to-your-network.

151 Kate O'Flaherty, 'SolarWinds: Microsoft Reveals New Details About Sophisticated Mega-Breach', *Forbes*, 16 February 2021, available at https://www.forbes.com/sites/kateoflahertyuk/2021/02/16/solarwinds-microsoft-reveals-new-details-about-sophisticated-mega-breach/.

152 Lukasz Olejnik and Tilman Rodenhäuser, 'Malware: A selection of essential cyber notions and concepts', *Humanitarian Law & Policy Blog* – ICRC, 23 May 2019, available at https://blogs.icrc.org/law-and-policy/2019/05/23/malware-essential-cyber-notions-concepts/.

153 Massimo Calabresi and Pratheek Rebala, 'Here's The Evidence Russia Hacked The Democratic National Committee', *TIME*, 13 December 2016, available at https://time.com/4600177/election-hack-russia-hillary-clinton-donald-trump/.

154 Zac Doffman, 'Russia Linked To Cyberattacks On Bellingcat Researchers Investigating GRU (Updated)', *Forbes*, 26 July 2016, available at https://www.forbes.com/sites/zakdoffman/2019/07/26/russian-intelligence-cyberattacked-journalists-hacking-encrypted-email-accounts/#3e2fa9cb12f4/.

155 Karspersky, 'What's the Difference between a Virus and a Worm?', available at https://www.kaspersky.com/resource-center/threats/computer-viruses-vs-worms.

destroy the host's programmes, as well as disrupt access, corrupt or destroy data.[156] They are usually spread through file exchange applications, downloaded files, email attachments, and USB drives.[157]

Conversely, worms do not need user activation or trigger to infect and self-propagate into the victim's computer or device – they are self-executable.[158] Moreover, they do not spread through executable files or applications, but by exploiting network vulnerabilities, such as missed operational system updates or software patches.[159] This means that they spread quickly across an entire network, including the Internet at large.[160] Worms are versatile types of malware: they can modify, delete or steal data, install additional malicious software, overload system resources, such as hard drive space or bandwidth, and install a backdoor, allowing the perpetrator to gain control over a computer and its system settings.[161]

f. Content-based cyber operations

We use the term 'content-based cyber operations' to cover activities which exploit the content layer of ICTs by generating and/or disseminating harmful content to users, including the victim and the general public. For present purposes, harmful content includes violent, discriminatory, misleading and false information. As this definition suggests, there is a multitude of content-based cyber operations already taking place on the Internet and other ICTs, and infinite possibilities remain in the way that digital content can be used to cause harm. In this report, we have selected three of the most recurrent

156 Cindy Ng, 'The Difference between a Computer Virus and Computer Worm', *Varonis Inside Out Security Blog*, available at https://www.varonis.com/blog/what-is-a-computer-virus-and-computer-worm/.

157 Ibid.

158 Kaspersky, 'What's the Difference?', *supra* note 155.

159 Kaspersky, 'Malware & Computer Virus Facts & FAQs', available at https://www.kaspersky.com/resource-center/threats/computer-viruses-and-malware-facts-and-faqs.

160 Varonis, *supra* note 156.

161 Norton, 'What is a computer worm, and how does it work?', 28 August 2019, available at https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html/.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

and harmful content-based cyber operations, which might be subject to a variety of international legal obligations: i) social engineering operations, such as phishing and biting; ii) cyber-enabled information operations, such as online mis and disinformation; iii) and online hate speech.

Social engineering operations or attacks are usually not an end in themselves, but part of a bigger operation in which they act as the gateway to malware and more harmful cyber operations. As their name suggests, those operations are based on human interaction, including human-to-human and machine-to-human, and the use of psychological manipulation to achieve malicious purposes.[162] In short, social engineering operations exploit human error rather than software or hardware vulnerabilities. And they are used in 98–99% of malware operations.[163] A prominent and recent example is the COVID-19 vaccine 'cold supply chain' attack. This attack was triggered by false email messages purporting to be from a reputable source and containing a malicious link which were sent to employees of companies that support the process of vaccine distribution around the world and are associated with the World Health Organisation's international vaccine alliance, i.e., Gavi's Cold Chain Equipment Optimisation Platform (CCEOP).[164] Social engineering operations may take a variety of forms, such as: i) phishing, which is the most common of its kind and consists of email or text messages aimed at obtaining credentials or attracting the victim to click on a malicious link or an attachment by causing fear, a sense of urgency or curiosity; ii) spear phishing, in which the phishing campaign targets specific individuals or organisations; iii) baiting, where the victim is lured to give in credentials, click on a malicious link or download malware by an offer of free goods, such as music downloads; and iv) pretexting, whereby the perpetrator gains a victim's trust and exfiltrates credentials or

162 Nate Lord, 'Social Engineering Attacks: Common Techniques & How to Prevent an Attack', *Data Insider*, 1 December 2020, available at https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack; Imperva, 'Social Engineering', available at https://www.imperva.com/learn/application-security/social-engineering-attack/.

163 Proofpoint, 'The Human Factor Report', 2019, available at https://www.proofpoint.com/us/resources/threat-reports/human-factor; Purplesec, *supra* note 108.

164 See *supra* notes 66 and 67.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

other personal information by creating a fabricated story which sounds trustworthy.[165]

While traditionally associated with war propaganda and other military psychological operations (often labelled as 'information warfare'), cyber-enabled information operations have gained renewed interest and prominence in war and peacetime with the advent of the Internet and social media platforms.[166] In the military context, these operations have aimed at influencing, disrupting, corrupting, or usurping the decision-making of adversaries, including combatants and civilians.[167] But beyond being a war tactic, they have become a common tool of social and political disruption in the hands of state and non-state groups. Like to social engineering operations, cyber-enabled information operations use true, misleading or false content or information to exploit or influence personal opinions, emotions and behaviour.[168] These operations normally take place in three so-called dimensions or planes, namely, i) the 'physical world', which refers to the use of hardware or computer devices and the tangible or non-tangible impact on organisations and individual; ii) the content or information dimension, which comprises the collection, processing, storage and dissemination of content and the flow of information between network users; and iii) the cognitive dimension, where the desired impact on human decision-making takes place on the basis of how information is perceived.[169] Cyber-enabled information operations may take a variety of forms, but their most common types are: i) online propaganda, that is, the dissemination or propagation of true, misleading or stolen ideas, information or narratives that intended to influence a group of individuals; ii) disinformation, i.e., the intentional manipulation or

165 Imperva, *supra* note 162; David Bisson, '5 Social Engineering Attacks to Watch Out For', *The State of Security*, 5 November 2019, available at https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/; Social Engineering Attacks, *IT Governance*, available at https://www.itgovernance.co.uk/social-engineering-attacks.

166 Accenture, '2019 Cyber Threat Landscape Report', *supra* note 52, at 13, 18-19; Gary Brown, 'Addressing Cyber-Enabled Information Operations', *RUSI*, 1 May 2020, available at https://rusi.org/sites/default/files/20200501_brown_web.pdf.

167 Catherine Theohary, 'Defense Primer: Information Operations', *US Congressional Research Service*, 15 December 2020, available at https://fas.org/sgp/crs/natsec/IF10771.pdf, at 1.

168 Accenture, '2019 Cyber Threat Landscape Report', *supra* note 52, at 13-14.

169 Theohary, *supra* note 167, at 1.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

influencing of individual or public opinion through false or misleading information, usually through false accounts or 'bots', known as 'trolls'; and iii) misinformation, which refers to the unintentional spreading or forwarding of misleading or false information by individuals or bots, usually on social media or through messaging applications.[170] Examples of orchestrated and highly disruptive mis- and disinformation operations are the recent conspiracy theories about coronavirus and the various COVID-19 vaccines spread on social media platforms.[171]

As indicated earlier, online hate speech can cause significant physical and psychological harm to individuals whilst causing social, political and cultural division in affected communities. 'Hate speech' is not a legal term of art and there is no single, unified definition to the term. Yet it is often used in general and expert discourse to refer to the oral or written dissemination of ideas that dehumanise or attack the dignity of groups or individuals belonging to a group, including by inciting hatred or violence against them.[172] Hate speech has been a constant, if not inescapable feature of mass atrocities committed at least since the 20th century, such as Armenian massacre in Turkey, the Holocaust, the ethnic cleansing campaign in the Former Yugoslavia and the Rwandan genocide.[173] In all those instances, derogatory language was disseminated on the mass media to create the circumstances conducive to violence. It eventually led to some of the most serious human rights abuses and atrocity crimes, such as genocide, war crimes and crimes against humanity. More recently, social media and other online platforms, such as private messaging applications, have been widely used as vehicles of hate speech, giving it an unprecedented dimension

170 Ibid; Accenture, '2019 Cyber Threat Landscape Report', *supra* note 52, at 15-20; Claire Wardle and Hossein Derakshan, 'Information Disorder: Toward an interdisciplinary framework for research and policymaking', Council of Europe Report, DGI(2007)09, 27 September 2017, available at https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c, at 5, 10-13, 20-21.

171 See *supra* note 75.

172 E.g., ARTICLE 19, '"Hate Speech" Explained: A Toolkit', 2015, available at https://www.article19.org/resources/hate-speech-explained-a-toolkit, at 9-14; HRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', 9 October 2019, A/74/486, para 1, including fn 1; United Nations Secretary General (UNSG), 'United Nations Strategy and Plan of Action on Hate Speech', May 2019, available at https://www.un.org/en/genocideprevention/documents/advising-and-mobilizing/Action_plan_on_hate_speech_EN.pdf, at 2; Susan Benesch, 'Dangerous Speech: A Proposal to Prevent Group Violence', 23 February 2013, available at https://dangerousspeech.org/wp-content/uploads/2018/01/Dangerous-Speech-Guidelines-2013.pdf, at 1.

173 See generally Gregory S. Gordon, *Atrocity Speech Law: Foundation, Fragmentation, Fruition* (Oxford University Press, 2017).

and impact.[174] It can and has led to life-threatening violence and, more generally, threats democratic values, stability and peace.[175] This impact has been recently put on the spotlight with Donald Trump's hateful rhetoric on Twitter, which likely incited the January 2021 US Capitol riots,[176] COVID-19-related online speech,[177] stigmatising and blaming groups for the consequences of the pandemic, well as the continuous expression of hatred and discrimination against the Rohingya people on social media platforms around the world.[178]

5. Different scenarios

The foregoing cyber operations and their ensuing harms may implicate different actors, including states, non-state groups and individuals, in a number of different scenarios to which international law, particularly protective obligations requiring states to prevent, stop or redress harm, might apply.

First and foremost, any such operations and harms may directly originate from one state's organs or entities and target another state's government, territory or population. This is a traditional state-to-state operation which depends on its attribution to the origin state under the customary rules reflected in Articles 5 to 11 of the International

174 HRC, *supra* note 172, para 1; UNSG, *supra* note 172, at 1.

175 NSG, *supra* note 172, at 1.

176 Graeme Massie, 'A timeline to insurrection: The Trump tweets that security experts say led to the Capitol riots', *The Independent*, 18 January 2021, available at https://www.independent.co.uk/news/world/americas/us-election-2020/trump-tweets-attacks-capitol-violence-b1786246.html; Ryan Goodman, Mari Dugas and Nicholas Tonckens, 'Incitement Timeline: Year of Trump's Actions Leading to the Attack on the Capitol', *Just Security*, 11 January 2021, available at https://www.justsecurity.org/74138/incitement-timeline-year-of-trumps-actions-leading-to-the-attack-on-the-capitol/; 'Capitol riots: Did Trump's words at rally incite violence?', *BBC News*, 14 February 20201, available at https://www.bbc.co.uk/news/world-us-canada-55640437.

177 Amina Ahmed, 'A Tsunami Of Hate': The Covid-19 Hate Speech Pandemic', *Human Rights Pulse*, 20 June 2020, available at https://www.humanrightspulse.com/mastercontentblog/a-tsunami-of-hate-the-covid-19-hate-speech-pandemic; Human Rights Watch, 'Covid-19 Fueling Anti-Asian Racism and Xenophobia Worldwide', 12 May 2020, available at https://www.hrw.org/news/2020/05/12/covid-19-fueling-anti-asian-racism-and-xenophobia-worldwide; United Nations, 'United Nations Guidance Note on Addressing and Countering COVID-19 related Hate Speech', 11 May 2020, available at https://www.un.org/en/genocideprevention/documents/Guidance on COVID-19 related Hate Speech.pdf; 'Statement by The Group of 77 and China on the Covid-19 Pandemic', 3 April 2020, available at https://www.g77.org/statement/getstatement.php?id=200403, para 8.

178 See *supra* note 87 and Human Rights Watch, 'Joint Letter Re: End Violent Threats and Anti-Rohingya Campaign - Violent Threats and "Hate Speech" against Rohingya Community in Malaysia', 11 May 2020, available at https://www.hrw.org/news/2020/05/11/joint-letter-re-end-violent-threats-and-anti-rohingya-campaign.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

Law Commission (ILC)'s Articles of Responsibility for Internationally Wrongful Acts.[179] However, unless the operation is openly carried out or endorsed by an official state organ or agent, which is rare, it will be extremely difficult to legally attribute it to a state. This is so for a number of reasons. In particular, the Internet has a decentralised architecture, which is based on user-anonymity and efficient but unpredictable Internet routes (see Figures 2 and 3).[180] This architecture, coupled with the rising use of spoofing or re-routing techniques,[181] which masque the origin of online communications, makes it factually difficult to identify the individual or entity behind a cyber operation, even if one can trace the IP address and territory from which it emanated.[182] In addition, the legal threshold for attributing the conduct of private entities or individuals to a state is very high and demanding, requiring complete dependence or effective control by the state vis-à-vis each particular operation.[183] Not surprisingly, this means that states tend to carry out harmful cyber operations through proxies.[184]

Given the difficulty to identify state-to-state cyber operations, at least legally or formally, many such operations take the shape of a private group or entity (whether or not supported by the host or territorial state) targeting individuals, objects or governmental entities in one or more foreign states.

179 ILC, Articles on Responsibility of States for Internationally Wrongful Acts, GA Res. 56/83 of 12 December (ARSIWA).

180 Laurence Lessig, *Code: Version 2.0* (Basic Books, 2006), at 236; 'Network Architecture', *The Things Network*, https://www.thethingsnetwork.org/docs/network/architecture.html. But see Ashwin J. Mathew, 'The myth of the decentralised internet', 5 *Internet Policy Review* (2016) 1-13.

181 VPNs have now become common place assets, a trend which has been further increased by the need for remote work during the COVID-19 pandemic. For e.g., according to Google trends, the global popularity of the search term "vpn" rose steadily over the past 10 years: https://trends.google.com/trends/explore?date=2011-02-09%202021-02-09&q=vpn, accessed 14 March 2021.

182 Jawwad A. Shamsi, Sherali Zeadally, Fareha Sheikh and Angelyn Flowers, 'Attribution in cyberspace: techniques and legal implications', 9 *Security and Communications Networks* (2016) 2886, at 2886-2887; Florian Skopik and Timea Pahi, 'Under false flag: using technical artifacts for cyber attack attribution', 8 *Cybersecurity* (2020) 1, at 6-7, 14; Panayotis A. Yannakogeorgos, 'Strategies for resolving the cyber attribution challenge', *Air Force Research Institute perspectives on cyber power*, December 2013, available at https://media.defense.gov/2017/May/11/2001745613/-1/-1/0/CPP_0001_YANNAKOGEORGOS_CYBER_TTRIBUTION_CHALLENGE.PDF, at 9, 13-16.

183 See Tomohiro Mikanagi and Kubo Mačák, 'Attribution of cyber operations: an international law perspective on the Park Jin Hyok case', 9 *Cambridge International Law Journal* (2020) 51, at 60-64

184 See generally Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge University Press, 2018); Jamie Collier, 'Proxy Actors in the Cyber Domain', 13 *St Antony's International Review* (2017) 25-47.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

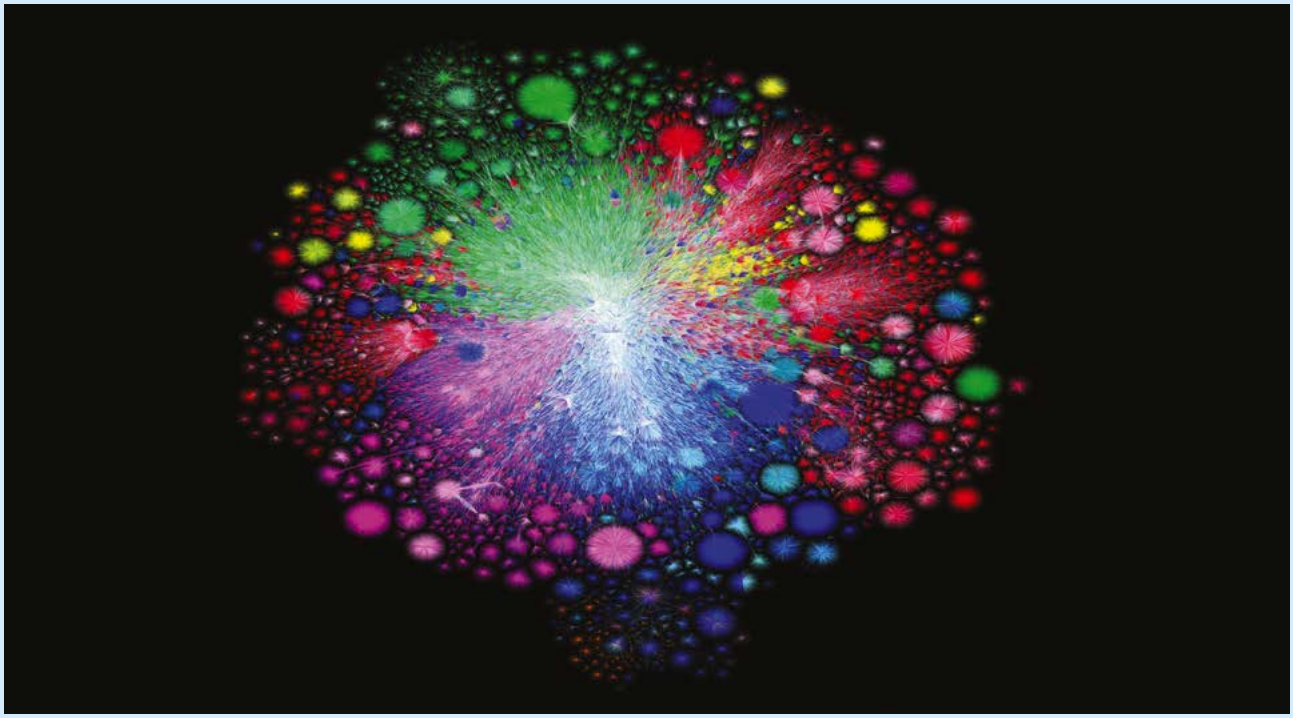

Figure 2: Map of the Internet's routes. The OPTE project. Key: White = Backbone; Blue = North America; Pink: Latin America; Red = Asia Pacific; Yellow = Africa; Green = Europe. Code by Barrett Lyon. Date: January 2021

Source: http://www.opte.org. Creative Commons Attribution License (reuse allowed).

Again, due to the decentralised architecture of the Internet, whose links cross multiple boundaries, it is often the case that cyber operations perpetrated by states or non-state entities transit through at least one third state before reaching their final destination. Transit, in this context, means the flow of data packets through routers, servers, and cables located in another state. This necessarily takes place if the information being accessed, i.e., received or sent, is stored in a computer server or host located abroad. As of June 2020, the highest concentration of Internet hosts could be found in North America, Europe and Japan,[185] with Google and Microsoft at the top of list of companies with most servers.[186]

185 Stackscale, 'All Internet servers together draw the world map', 01 June 2020, available at https://www.stackscale.com/blog/internet-servers-map/.

186 WhoIsHostingThis Team, 'Where in the World Does the Internet Live?', 28 September 2020, available at https://www.whoishostingthis.com/blog/2013/12/06/internet-infographic/.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

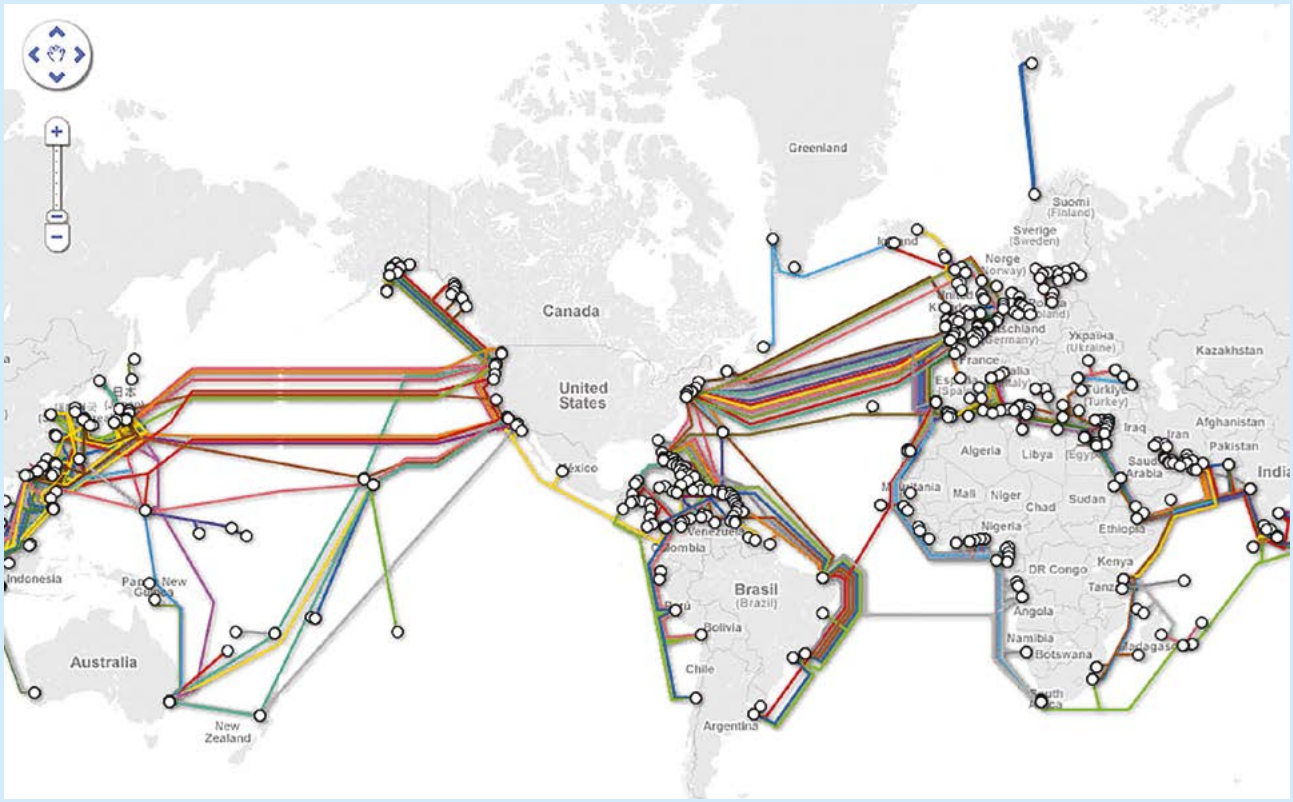

Figure 3: World map of submarine communication cables. TeleGeography, 28 July 2021.
Source: *https://www.submarinecablemap.com*

At the same time, we may also find purely or primarily domestic scenarios, where an individual or group located in one state targets objects, individuals or entities located in the same state, usually using links and routers located in the same state or satellite connection.

And it is important to bear in mind that, in these various scenarios, harms caused in a state's territory rarely only affect governmental entities but likely impact upon the rights of private entities, including, in particular, individuals and corporations.

What should states be protecting from? A taxonomy of cyber harms and the relationships they engage

6. Conclusion: The landscape of present and future ICT threats

Even if we remain sceptical as to the possibility of a 'cyber doomsday', i.e. one or more cyber operations leading to world-wide global shock, the current ICT landscape is already marked by a variety of harmful cyber harms affecting software, hardware, data and, most importantly, natural and legal persons. As the international community becomes all the more dependent on ICTs, its vulnerability to malicious cyber activity grows in surface.

Various classifications have been devised for cyber operations and the harms that arise from them. However, for the purposes of assessing the application of international law to ICTs, we find that a helpful taxonomy of cyber harms is to divide them into the ICT layers that they affect – hardware, software, data and persons. In the same vein, based on the quality or attribute that these operations compromise, existing and potential harms spam breaches of confidentiality, integrity and availability of hardware, software and data, as well as tangible and non-tangible damage on natural and legal persons.

Different types of cyber operations affect one or more of those layers in multiple ways, and they include (D)DoS attacks, ransomware, spyware, RATs, viruses, worms and content-based operations. We concluded that whether or not they are carried out by exploiting vulnerabilities in hardware, software, data or people, their impact on individuals is real. These may be carried out by states or non-state groups and might well transit through others states before targeting individual or governments abroad.

The sheer variety and impact of cyber harms calls for greater emphasis on their prevention and mitigation. As we shall see in the following chapters, international law is not indifferent to this state of affairs. Whether or not cyber wars and catastrophes loom on the horizon, several rules of international law require states to prevent, stop and redress cyber harms.

Sovereignty and jurisdiction over ICTs

1. Introduction

Any analysis of states' protective duties in cyberspace and beyond would not be complete without recalling the foundation on which such duties are built, i.e., the concept of state sovereignty. When it comes to interpreting rules of international law applicable to ICTs, in this report especially with respect to protective obligations establishing a due diligence standard, sovereignty and the related concept of jurisdiction play a double role. On one side, they identify the duty-bearer of those obligations, the sovereign entity with responsibility for preventing, halting and redressing the relevant harmful cyber operations. On the other side, sovereignty and jurisdiction impact the extent to which a State is protected against foreign incursions on its own cyber infrastructure. The following two sections will expand on this double function, by focusing first on delineating States' sovereign rights and duties in the use of ICTs, and secondly on States' jurisdictional reach in cyberspace.

2. Sovereign Rights and Duties over ICTs

Sovereignty is often meant to designate 'the whole body of rights and attributes which a state possesses in its territory, to the exclusion of all other states, and also in its relations with other states.'[1] In the relations between states, sovereignty is also described as 'independence in regard to a portion of the globe', that is, 'the right to exercise therein, to the exclusion of any other State, the functions of a State'.[2] As such, sovereignty is the defining feature of statehood and commonly associated with the authority and power which a state wields in its internal and external relations.[3]

1 Individual Opinion by Judge Alvarez in *Corfu Channel Case* (United Kingdom v Albania), Judgment, 9 April 1949, ICJ Reports (1949) 39, at 43.

2 *Island of Palmas Case (or Miangas), United States v Netherlands*, Award, 4 April 1928, II RIAA 829 (1928), ICGJ 392 (PCA 1928), at 838. Cf. Samantha Besson, 'Sovereignty', *Max Planck Encyclopaedia of Public International Law (MPEPIL)* (2011), available at https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1472?prd=EPIL, para. 70; and Gary P. Corn and Robert Taylor, 'Sovereignty in the Age of Cyber', 111 *AJIL Unbound* (2017) 207-212, at 209.

3 Cf. Individual Opinion of Judge Anzilotti in *Customs Regime between Germany and Austria*, Advisory Opinion, 5 September 1931, 1931 P.C.I.J. (ser. A/B) No. 41 (Sept. 5), at 57; Besson, *supra* note 2, para. 56. However, it is to be noted that sovereignty is still primary territorial: see *Island of Palmas*, *supra* note 2, at 838-839.

Sovereignty and jurisdiction over ICTs

Whilst state sovereignty is often implied to be a value in itself, which must be 'protected' by international law, it has been persuasively and perhaps more accurately conceptualized as being 'defined' by international law.[4] According to such view, sovereignty is a means to achieve the very goal of statehood, i.e. the well-being of society, manifested through the full enjoyment of human rights internally and the peaceful coexistence of nations externally.[5] Thus, rights and duties characterising a sovereign entity, which are established by international law, are 'functionally' aimed at the realisation of the abovementioned goal.[6] On this reading, limitations to a state's sovereignty derive first and foremost from the need to preserve the attributes of other states, equally sovereign, as well as the need to protect individuals therein.

Indeed, the view that sovereignty entails not only rights but also obligations that seek to safeguard other states and human beings has been long recognised by international courts and tribunals. For instance, in the *Island of Palmas* case, the Arbitral Tribunal concluded that:

> This right [to territorial sovereignty] has as corollary a duty: the obligation to protect within the territory the rights of other States, in particular their right to integrity and inviolability in peace and in war, together with the rights which each State may claim for its nationals in foreign territory. Without manifesting its territorial sovereignty in a manner corresponding to circumstances, the State cannot fulfil this duty. Territorial sovereignty cannot limit itself to its negative side, i.e., to excluding the activities of other States; for it serves to divide between nations the space upon which human activities are employed, in order to assure them at all points the minimum of protection of which international law is the guardian.[7]

4 Anne Peters, 'Humanity as the A and Ω of Sovereignty', 20 *European Journal of International Law* (EJIL) (2009) 513–544, at 520-521, citing Fassbender, 'Sovereignty and Constitutionalism in International Law', in N. Walker (ed.), *Sovereignty in Transition* (2003), at 115, 129. Similarly, Besson, *supra* note 2, especially at para 109: 'What a State's sovereignty is and what it amounts to is not given as a matter of the intrinsic value of its individuality but determined by the rules of the international legal order. Those rules define State sovereignty so as to protect the internal and external interests and values of the political community qua sovereign equal to others, but also to protect the interests of their subjects.'

5 Cf. Peters, *supra* note 4, especially at 518-522. See also Besson, *supra* note 2, at paras 31-32.

6 Cf. Peters, *supra* note 4, at 518-522. See also Besson, *supra* note 2, at para. 46: 'modern international sovereignty … became a function distinct from the legal persona of the State'.

7 *Island of Palmas*, *supra* note 2, 839.

Sovereignty and jurisdiction over ICTs

As clarified by the UN GGE, 'State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT related activities and to their jurisdiction over ICT infrastructure within their territory.'[8] In the same vein, the Tallinn Manual 2.0 begins precisely by affirming that '[t]he principle of State sovereignty applies in cyberspace',[9] and then follows suit by clarifying that each state 'enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations'[10] and 'is free to conduct cyber activities in its international relations, subject to any contrary rule of international law binding on it.'[11]

Yet two diverging approaches have emerged with respect to the transliteration of the notion of sovereignty from the offline to the online environment. A first approach bestows configurations of sovereign authority and power, which are usually linked to territorial spaces and cyber activities taking place somewhere.[12] There are variants to this approach, which one may label as 'territorialisation' of cyberspace, depending on whether such configurations of authority and power are only extended to cyber infrastructure and processes (i.e. the physical and logical layers of cyberspace) or whether they are also extended to data (i.e. the content layer).[13]

A second approach, which could be labelled as 'de-territorialisation' of cyberspace, posits instead that authority and power over ICTs —

8 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security ('UN GGE Report 2015'), 22 July 2015, UN Doc. A/70/174, para. 27. See also Wolff Heintschel von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace', 89 *International Legal Studies* (2013) 123, at 126.

9 Michael Schmitt (ed.), *Tallinn Manual 2.0* on the International Law Applicable to Cyber Operations (Cambridge University Press, 2017), at 11, Rule 1.

10 Ibid., at 13, Rule 2.

11 Ibid., at 16, Rule 3.

12 What Henning Lahmann refers to as 'Cyber Westphalia', in 'The Politics and Ideologies of the Sovereignty Discourse in Cyberspace', paper presented at the ESIL Krakow Symposium on 'Exploring the Frontiers of Cyberspace, 4 December 2020 (on file with authors), Section 3. See also Daniel Lambach, 'The Territorialization of Cyberspace', 22(3) *International Studies Review* (2020) 482-506, at 488-489; and Darrel C. Menthe, 'Jurisdiction in Cyberspace: A Theory of International Spaces', 4 *Michigan Telecommunications and Technology Law Review* (1998) 69, at 79. With reference to, e.g., Chinese practice, see Rogier Creemers, 'China's Conception of Cyber Sovereignty: Rhetoric and Realization', in Dennis Broeders, Bibi van den Berg (eds), *Governing Cyberspace: Behavior, Power, and Diplomacy* (Rowman & Littlefield, 2020) 107, at 116.

13 The latter seems to be the approach espoused in the *Tallinn Manual 2.0*, *supra* note 9, at 12 and 15-16, Rule 1, paras 4 and 11, and at 63, Rule 10, para. 8.

Sovereignty and jurisdiction over ICTs

especially expressed in the form of regulation of cyber activities — are detached from a specific territory.[14] This approach, on the one hand, seems to more closely reflect the reality of modern international cyber relations, in which power is not wielded exclusively by states but also by diverse non-state norm-setting authorities (e.g. the Internet Corporation for Assigned Names and Numbers, or ICANN, a US multistakeholder group and non-profit organization responsible for managing, among other things, the Internet's Domain Name Systems), with multiple sources of normativity and a plurality of norm addressees.[15] On the other hand, this 'deterritorialization' approach may justify recognising that states' regulatory and perhaps enforcement powers, as well as their obligations have an extraterritorial reach.[16]

In light of the above, and of its 'original' role with respect to most rules of international law, the chosen approach to 'digital' sovereignty, or sovereignty over ICTs, significantly influences the interpretation and implementation of several international rules applicable to cyber operations, including, in particular, obligations requiring states to prevent, halt and redress harm.

On one side, the notion of sovereignty is crucial to delineate the protection to which states are entitled *against* external intrusions and/or interference, that is, states negative obligations vis-à-vis other states and individuals. In other words, the extent of sovereignty determines whether the protection of states and individuals from certain cyber operations only covers the physical and logical layer of their infrastructure, or also the content layer, will depend on the particular reading of sovereignty adopted. This, in turn, will determine what kinds of cyber operations may be unlawful and, thus, must be prevented, halted and redressed under international law.

14 Lambach, *supra* note 12, at 491 ff., defining (at 492) the practice of deterritorialization as 'the dissolution, erosion, or destruction of old territorial forms of organizing social relations', and observing how it is usually accompanied by practices of 'reterritorialization'.

15 Talking about 'corporate territories' Lambach, *supra* note 12, at 498-499. On the role of ICANN, among other private entities, see Joachim Zekoll, 'Jurisdiction in Cyberspace', in Günther Handl, Joachim Zekoll and Peer Zumbansen, *Beyond Territoriality: Transnational Legal Authority in an Age of Globalization* (Martinus Nijhoff, 2012) 341, at 357ff.

16 As described, e.g., in Lahmann, *supra* note 12, Section 2, where the author describes the practice as leading to 'cyber imperialism', as evidenced by the US approaches like 'defend forward' and 'persistent engagement'.

Sovereignty and jurisdiction over ICTs

On the other, understanding the boundaries of sovereignty determines the scope of states' positive duties to safeguard other states and individuals from malicious cyber operations. That is, sovereignty defines not only *when* a state is expected to prevent and respond to such operations but also the *extent* to which such state is bound in its effort to do so, i.e., what behaviour may be considered 'diligent' so as discharge the obligation in question. Simply put, the proper interpretation and implementation of rules flowing from sovereignty underlie the peaceful co-existence of several 'digital' sovereigns: they establish the measure to which a state is entitled to freedom from external interference and the actions which, instead, it must tolerate or undertake.

In the past few years, debates over what kind of 'cyber' interferences are prohibited or which action must be tolerated or taken have reached an impasse. Whilst there is general agreement that the use of force and coercive intervention in a state's internal affairs by cyber means are both prohibited,[17] more controversial is the view that a 'residual' primary rule of international law (rooted in territorial sovereignty) protects states' ICT infrastructure, including their physical, logical and content layers, against intrusion by other states. Whereas some states have taken an ambiguous stance on the question,[18] the United Kingdom has firmly opposed such a rule.[19] In contrast, other states expressed variously nuanced positions in favour of the existence of a rule protecting states' territorial sovereignty over cyber infrastructure, that is, their right to exercise authority over such infrastructure to the exclusion of other subjects.[20] Such rule is reflected in one of rules

17 Cf. UN GGE Report 2015, *supra* note 8, para 26; see also Corn and Taylor, *supra* note 2, at 208; and Harriet Moynihan, 'The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention', *Chatham House Research Paper* (2020), at 26-36.

18 E.g. the United States, as discussed in Przemysław Roguski, 'Application of International Law to Cyber Operations: A Comparative Analysis of States' Views', *The Hague Program For Cyber Norms Policy Brief* (March 2020), at 6.

19 UK Attorney General Jeremy Wright, 'Speech: Cyber and International Law in the 21st Century', 23 May 2018, available at https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

20 E.g. France, affirming that '[a]ny cyber attack against French digital systems or any production of effects on French territory via digital means by [a State or a State-sponsored entity] constitutes a violation of sovereignty', in 'International Law Applied to Operations in Cyberspace', 2019, available at https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf, at 7. For a comparative analysis of positions expressed by France, the Netherlands and Germany, see Roguski, *supra* note 18, at 5-6. See also Przemysław Roguski, 'Iran Joins Discussions of Sovereignty and Non-Intervention in Cyberspace', *JustSecurity*, 3 September 2020, at https://www.justsecurity.org/72181/iran-joins-discussions-of-sovereignty-and-non-intervention-in-cyberspace/.

Sovereignty and jurisdiction over ICTs

articulated in the Tallinn Manual 2.0 which states that each state has a duty not to 'conduct cyber operations that violate the sovereignty of another State.'[21]

Even for those who accept such a rule, the question remains as to what particular cyber operations — if carried out by remote means — would violate state sovereignty. Among the Group of Experts who drafted the Tallinn Manual 2.0, there was agreement that cyber operations resulting in physical damage or injury or loss of functionality (such as those necessitating repair, replacement or reinstallation of data) would qualify,[22] as would those interfering or usurping inherently governmental functions of another state, irrespective of damage or loss of functionality.[23] However, no consensus was reached on other matters, for instance as to the exact meaning of 'loss of functionality', and whether a violation of sovereignty could materialise in operations below this threshold.[24] Understanding the exact contours of this rule may help us to identify cyber operations which qualify as 'harmful' and thereby delineate the scope of protective, 'due diligence', obligations.

That being said, thus far, discussions on a rule protecting sovereign rights over ICT infrastructure seem to have neglected at least two considerations. The *first* consideration is that a state may have to tolerate interferences with its own sovereign rights when these are justified by the lawful exercise of the rights of another sovereign over ICTs. This may be expressed, for instance, in interferences which are justified by a valid title of jurisdiction. *Second*, asserting sovereignty over ICTs not only entitles a state with rights but also places on it duties and corresponding responsibilities. Among these, one may recall the duties to protect and ensure the human rights of individuals who are under a state's sovereign authority, i.e., under its jurisdiction. Given the centrality of jurisdiction to both considerations, it is to this concept which we now turn.

21 *Tallinn Manual 2.0*, *supra* note 9, at 17, Rule 4.

22 Ibid., at 20-21, Rule 4, paras 11-13.

23 Ibid., at 21-23, Rule 4, paras 15-22.

24 Ibid., at 21, Rule 4, para. 14.

3. The Jurisdiction of Sovereigns over ICTs

The ensemble of rights and obligations which characterise sovereignty finds concrete expression in a state's power over persons, objects and events. This exercise of state authority, which may assume different forms, is often referred to as jurisdiction.[25] In this sense, jurisdiction can be conceptualised not only as a corollary, but as the very 'projection' or 'operationalisation' of the notion of state sovereignty.[26]

Etymologically, 'jurisdiction' originates in the Latin expression *juris dicere*, describing the condition of those who 'say what the law is', that is, those tasked with interpreting it in a dispute or in charge of enforcing it.[27] In this ancient concept, one may find the roots of the modern understanding of the three dimensions of prescriptive, adjudicative and enforcement jurisdiction.

Thus, jurisdiction is the basis of every 'relational' rule binding on a state, that it, all state obligations vis-à-vis other states and individuals. 'Having jurisdiction' may be understood as meaning 'projecting state authority' over persons (including users of digital technology), objects (including a territory and infrastructure therein located) or events (including a particular cyber operation or incident). Such projected state authority takes typically (but not exclusively) the form of the prescription of laws and regulations, their adjudication and enforcement.[28]

25 Cf. slightly differently worded but similar definitions in Bernard H Oxman, 'Jurisdiction of States', *MPEPIL* (2007), available at https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1436, para. 3; James Crawford, *Brownlie's Principles of Public International Law* (8th edn., Oxford University Press, 2012), at 456. See also Malcolm N. Shaw, *International Law* (8th edn., Cambridge University Press, 2017), at 483; and Christopher Staker, 'Jurisdiction', in Malcolm D. Evans (ed.), *International Law* (4th edn., Oxford University Press, 2014) 309, at 309. With reference to cyberspace, see also *Tallinn Manual 2.0*, *supra* note 9, at 51, Rule 8 and accompanying commentary.

26 Cf. Peters, *supra* note 4, at 516.

27 Cf. Cedric Ryngaert, *Jurisdiction in International Law* (OUP 2015), at 5, citing Joseph Plescia, 'Conflict of Laws in the Roman Empire' 38 *Labeo* (1992) 30, at 32.

28 Cf. Oxman, *supra* note 25, paras 1 and 3; Ryngaert, *supra* note 27, at 9; Roger O'Keefe, 'Universal Jurisdiction: Clarifying the Basic Concept', 2 *Journal of International Criminal Justice* (2004) 735, at 736-737.

Sovereignty and jurisdiction over ICTs

Within this framework, rules of international law govern state jurisdiction by establishing certain 'links', 'titles' or 'grounds' — e.g. a spatial relationship centred on the territorial location of the person/object/event; or a personal relationship, based on an individual's nationality.[29] These seek to limit the number of circumstances in which each state is lawfully allowed to 'project' or exercise its own rights or authority, and, at the same time, the scope or extent of its duties vis-à-vis other states and individuals. In so doing, the rules of international law governing state jurisdiction seek to ensure the co-existence of several entities wielding sovereign power.[30]

Whilst the majority decision in the *Lotus* case famously held that restrictions on sovereign power cannot be presumed,[31] several rules of international law precisely establish such restrictions by determining when a state does or does not have jurisdiction. If one accepts that the notion of state sovereignty implies not only power (rights) but also responsibility (duties), it follows that 'having jurisdiction' means not only having rights but also duties to act in a certain way, with respect to a certain object, person or event.[32] It is precisely this notion of jurisdiction that delineates the protective obligations analysed in this report: the establishment of state jurisdiction under international law carries with it a number of duties to behave diligently in preventing, halting and/or redressing certain harms. This is in line with the aforementioned idea that sovereignty is a means for states to achieve the well-being of individuals and societies, rather than an end in itself.

It is generally understood that a state has (or 'possesses') jurisdiction — and can exercise it in the prescriptive, adjudicative and enforcement forms — over persons, objects or events located *within its borders*.[33]

29 Cf. Oxman, *supra* note 25, paras 10ff.

30 Cf. Oxman, *supra* note 25, para 9.

31 *The Case of the S.S. Lotus*, 1927 PCIJ Series A, No. 10, at 18.

32 This is the case, for instance, for human rights obligations. See e.g. Ryngaert, *supra* note 27, at 22-23. It is also the case for the other protective obligations analysed in Chapter 4 of this report.

33 Oxman, *supra* note 25, para 11; Jan Klabbers, *International Law* (2nd edn., Cambridge University Press, 2017), at 100. Andrew B. Clapham, *Brierly's Law of Nations: An Introduction to the Role of International Law in International Relations* (7th edn., Cambridge University Press, 2012), at 242. With reference to cyberspace, see *Tallinn Manual 2.0*, *supra* note 9, at 55, Rule 9 and accompanying commentary.

Sovereignty and jurisdiction over ICTs

Conversely, in order to favour the peaceful co-existence and uphold the equality of different sovereigns, the extent of a state's jurisdiction *outside of its borders* (also known as 'extraterritorial' jurisdiction) is comparatively narrower.[34] International law governs the circumstances in which a state possesses extraterritorial jurisdiction: in those limited cases, the state in question is allowed to encroach upon the sovereign prerogatives of other states, which in turn must tolerate such restriction on their own rights, internally or externally.[35]

Oftentimes, states may invoke grounds to exercise prescriptive jurisdiction extraterritorially.[36] Two examples, in the cyber context, are *i)* the enactment of legislation for cybercrimes perpetrated abroad;[37] or *ii)* the adoption of technical regulations for digital products and services developed by foreign companies seeking to access the host state's market.[38] The same cannot be said for enforcement jurisdiction, since the general rule in this regard is that a state may not exercise enforcement powers on the territory of other states without their consent.[39] For instance, it may be more difficult to find a valid title of jurisdiction for conducting law enforcement or other operations on ICT infrastructure located outside of a state's territory, even if it is

34 Oxman, *supra* note 25, para 51; Menno T. Kamminga, 'Extraterritoriality', *MPEPIL* (2020), available at https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1040?rskey=RBqjN9&result=1&prd=OPIL, paras 2-3. See also *Tallinn Manual 2.0*, *supra* note 9, at 52, paras 4-5 and 8.

35 See Kamminga, *supra* note 34, paras 7 and 10; and *Tallinn Manual 2.0*, *supra* note 9, at 61, Rule 10, paras 2-3. For instance, with respect to the exercise of 'effects-based jurisdiction with respect to cyber-related activities and the persons who engage in them', the Tallinn Manual 2.0 (which discusses it under territorial jurisdiction, but acknowledges its special status) lists some 'generally recognised conditions' including: 'that the State which enacts effects-based legislation has a clear and internationally acceptable interest in doing so; that the effects which it purports to regulate must be sufficiently direct and intended or foreseeable; that those effects must be substantial enough to warrant extending the State's law to foreign nationals outside its territory; and that the exercise of effects-based jurisdiction does not unduly infringe upon the interests of other States, or upon foreign nationals, without a significant connection to the State that purports to exercise such jurisdiction.' See *Tallinn Manual 2.0*, *supra* note 9, at 58, Rule 9, para. 13.

36 Kamminga, *supra* note 34, para 9. The author cautions, however, the resort to any of these grounds does not automatically mean that the exercise of jurisdiction in question is lawful under international law. As a matter of fact, the interpretation of jurisdictional grounds such as the protective principle or the effects doctrine may vary greatly across different States. Some of these grounds also overlap with each other. See Ibid., paras 10 and 16.

37 As requested, e.g., by the 2001 Budapest Convention. Cf. von Heinegg, *supra* note 8, at 126. See also (though discussing this example under the 'effects doctrine', as part of territorial jurisdiction) *Tallinn Manual 2.0*, *supra* note 9, at 59, Rule 9, paras 15-17.

38 Which could be based both on the 'effects doctrine' (see *supra* note 35) or, if the products and services are likely to affect vital interests of the State, on the protective principle. On the latter, see *Tallinn Manual 2.0*, *supra* note 9, at 63-64, Rule 10(c), paras 10-12.

39 *Tallinn Manual 2.0*, *supra* note 9, at 66ff., Rule 11. See also Kamminga, *supra* note 34, para. 8, citing *Lotus*, *supra* note 31, at 18-19.

Sovereignty and jurisdiction over ICTs

allegedly being used by criminals to commit crimes therein.[40] Similarly, it may be hard to establish the existence of a valid title of jurisdiction for accessing data stored in another state[41] — though a state may have at least prescriptive and adjudicative powers over such data if it is in possession of a national entity, such as company incorporated in its territory, as in this case the jurisdictional ground of active nationality could be invoked.[42]

As a matter of fact, states hold differing views as to the extent of their jurisdiction with respect to cyber operations and ICTs.[43] Likewise, in light of the growing de-territorialized approach to state sovereignty in cyberspace and of the various jurisdictional grounds which may be in play, it may at times be hard to distinguish territorial from extraterritorial enforcement.[44]

Whilst these are general considerations, the exact extent of a state's jurisdiction can only be determined by reference to different rules of primary international law which govern it. In particular, transnational crime treaties, international and regional human rights conventions, international humanitarian law treaties, alongside relevant rules of customary international law, govern the circumstances in which a state has or lacks jurisdiction, and determine the rights and duties which flow from such jurisdiction. For this reason, this report analyses issues of jurisdiction separately, and more specifically, with respect to each of the different sets of protective obligations identified. In particular, jurisdiction within the framework of international human rights law receives, in this report, special attention due to the wealth of jurisprudence which has been produced on it, in particular by the European Court of Human Rights.

40 *Tallinn Manual 2.0*, *supra* note 9, at 68, Rule 11, para. 7.

41 Ibid., at 70, Rule 11, paras 15-17.

42 Ibid., at 61-62, Rule 10(a), paras 4-6.

43 Cf. Oxman, *supra* note 25, paras 31-32.

44 *Tallinn Manual 2.0*, *supra* note 9, at 69-70, Rule 11, paras 12-14.

Sovereignty and jurisdiction over ICTs

At this point, however, it may already be noted that certain rules of international law concerning the exercise of state jurisdiction are premised on the requirement of state 'control' over a territory or area, persons, objects or their attributes.[45] Likewise, different rules require different levels of control for jurisdiction to arise, such as 'effective' control or *de jure* authority.[46]

When it comes to ICTs, a number of complexities are added to the picture. First, whilst certain ICT layers, such as hardware, are necessarily physically located in a given space, the same cannot be easily said for other layers, such as software and data, which are reliant on physical infrastructure spread across multiple state borders.[47] Secondly, due to the interconnected nature of the Internet and other ICTs, and their very function of enabling one to exercise remote control over different devices, the exercise of control may not necessarily take a physical or material shape, transcending national borders or traditional conceptions of physical spaces.[48] Thirdly, whilst power and authority 'offline' are traditionally reserved to states, 'online' they are also wielded by a number of non-state entities, which complicates the identification of who has 'control' over a given person, object or event.[49] The said complexities may give rise to challenges when competing jurisdictional claims are based on control

45 For instance, Rule 6 of Tallinn Manual 2.0 establishes that a State must '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' (emphasis added). See *supra* note 9, at 30. With respect to human rights law, see e.g., Human Rights Committee (HRC), 'General comment no. 31 [80], The nature of the general legal obligation imposed on States Parties to the Covenant', 26 May 2004, UN Doc. CCPR/C/21/Rev.1/Add.13, para. 10.

46 E.g. 'Report of the Office of the UN High Commissioner for Human Rights: The Right to Privacy in the Digital Age', 30 June 2014, UN Doc A/HRC/27/37, para. 34, establishing the existence of jurisdiction whenever the State in question exercises 'effective' control over digital communications infrastructure. See also, as examples referred to personal jurisdiction for the purposes of IHRL, Inter-American Commission on Human Rights (IAComHR), *Coard et al. v. United States*, Report N. 109/99, 29 September 1999, para 37; ECtHR, *Al-Skeini and others v. United Kingdom*, Appl. no 55721/07, Judgment of 7 July 2011, paras 136-139. See also, proposing a functional reading of 'control' over the enjoyment of the rights in question, regardless of any *physical* control over territory, the perpetrators or the individual victim, HRC, '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, UN Doc. CCPR/C/GC/36, para. 63.

47 As noted in the discussion about the extent of territorial jurisdiction by the Group of Expert who drafted the Tallinn Manual 2.0. See *Tallinn Manual 2.0*, *supra* note 9, at 55, Rule 9, para. 3.

48 As aptly put by von Heinegg, *supra* note 8, at 140: 'the Internet's functionality—the benefits it provides—would be seriously challenged if States do not exercise their jurisdiction "with respect for one an-other's networks and the broader Internet."'

49 Lambach, *supra* note 12, at 498-499.

over data, software, hardware and persons.[50] While we touch on the notion of remote control in the context of different protective rules of international law, the question of how to solve conflicts of jurisdiction, in these instances, is beyond the scope of this report.

Finally, a word is warranted on the difference between, on one side, the notion of 'control' which — in application of specific rules of international law — triggers the existence of state jurisdiction; and, on the other side, the notion of 'capacity to influence' a source of harm which determines what the state is expected to do once jurisdiction is triggered (i.e. the extent to which it may be said to be behaving diligently).[51] The two concepts undoubtedly overlap, but the former is a pre-requisite for the latter, in a two-step process. The *first* step is understanding whether the state has jurisdiction and, thus, a duty to act: this assessment relies at times, as explained above, on whether the state has the relevant level of control over a certain person (e.g. the beneficiary of the protective duty or the perpetrator of the harm) or over a certain space (e.g. the territory from which a harm emanates or where it is producing effects). It is only once the existence of state jurisdiction is established that the protective duty kicks in, and the behaviour expected of the state — including what measures it must adopt — will depend on its capacity to act, including its capacity to influence the source of harm.[52]

4. Conclusion

As the primary subjects of international law, states not only have rights vis-à-vis other states but also duties that seek to give effect to their functions in the international community, i.e. to ensure the peaceful coexistence among sovereigns and the well-being of individuals. The

50 As noted in *Tallinn Manual 2.0*, *supra* note 9, e.g. at 52, Rule 8, para 7; and at 56-57, Rule 9, para 6-7. For proposed solutions, see Dan Jerker B. Svantesson, *Solving the Internet Jurisdiction Puzzle* (OUP 2017).

51 See *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 430.

52 The distinction between the two is also noted in Samantha Besson, 'Due Diligence and Extraterritorial Human Rights Obligations – Mind the Gap!', 9:1 *ESIL Reflections* (2020) 2, at 2.

Sovereignty and jurisdiction over ICTs

obligation to refrain from violating the rights of other states is the most obvious way to achieve that. Nevertheless, refraining from carrying out wrongful conduct is not enough. With great sovereign powers over a territory and population comes the great responsibility to ensure that the former is not used to harm other states and that that the latter's human rights are respected. In other words, duties to prevent and redress harm to other states and individuals are a corollary of state sovereignty and extend as far as a state's control or jurisdiction goes. To meet those obligations states must use their available powers under international law. While they can and must legislate, adjudicate and enforce laws domestically, the extent of their extraterritorial powers is limited by how international law shapes prescriptive and adjudicative jurisdiction outside national borders.

In the ICT environment, it remains unclear whether states have sovereign powers beyond infrastructure and persons physically located in their own territory to cover data and software elsewhere but which they own or control remotely. It is also unclear what acts undermine a state's sovereign rights over ICTs and whether these can breach international law. Although questions continue to surround the scope of state sovereignty and jurisdiction over ICTs, it is beyond doubt that, in the exercise of their existing jurisdictional powers over persons, objects or events, they must use ICTs with due care, doing what they can not to harm and to protect other states and individuals. What this duty of prevention or diligence entails exactly is a separate question, to which we turn next.

Due diligence in international law and its applicability to ICTs

Due diligence in international law and its applicability to ICTs

1. Introduction

Due diligence has recently become a buzz word in the 'cyber domain'. 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 of great uncertainty and increased cyber threats, due diligence features as a promising route to accountability, peace and security in cyberspace: it requires states to do employ their best efforts to prevent, halt and redress 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 their use of ICTs, including their physical, logical, content and personal layers.[3] On the one hand,

1 Russell Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm', 21 *Journal 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", 30 April 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', 22 May 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', 22 May 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', 22 May 2020, available at https://vm.ee/sites/default/files/Estonia_for_UN/statement_of_poland_arria_un_sc_on_cyber_22.05.2020.pdf, at 1; and 'Italy's statement at the Arria Formula Meeting on CYBER STABILITY, CONFLICT PREVENTION AND CAPACITY BUILDING', 22 May 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 Clare Sullivan, 'The 2014 Sony Hack and the Role of International Law', 8 *Journal of National Security Law and Policy* (2015) 437, at 454, fn 88. See also Nicholas Tsagourias, 'The Legal Status of Cyberspace', in Nicholas Tsagourias and Russell Buchan (eds.), *Research Handbook on International Law and*

Due diligence in international law and its applicability to ICTs

the 2015 GGE report, adopted by consensus by the UN General Assembly,[4] indicates that states '*should* not knowingly allow their territory to be used for internationally wrongful acts using ICTs.[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 a 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] On their face, these views seem irreconcilable and neither of them has gone unchallenged.[8]

We contend that the current debate misses the point by focusing too much on the meaning of 'due diligence' and its applicability to cyberspace. This has resulted in binary, 'all-or-nothing' views: either

Cyberspace (Edward Elgar, 2015) 13; David R. Johnson, David Post, 'Law and Borders: The Rise of Law in Cyberspace', 48 *Stanford Law Review* (1996) 1367.

4 GA Res. 70/237, 30 December 2015, para. 1-2(a).

5 '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/70/174, 22 July 2015 ('UN GGE Report 2015'), para. 13(c).

6 Michael Schmitt (ed.), *Tallinn Manual 2.0* (Cambridge University Press, 2017), at 30, Rule 6, and at 43, Rule 7.

7 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 the legal basis of this rule, recognizing its advantages but also warning about its drawbacks. See Eric T. Jensen and Sean 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 Liisi 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, para. 12. At least three States (Argentina, Israel, New Zealand) have expressed scepticism about the rule: see 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], 11 February 2020, available at http://webtv.un.org/search/4th-meeting-open-ended-working-group-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-second-substantive-session-10%E2%80%9314-february-2020/6131734500001/?term=%22Open%20Ended%20Working%20Group%22&lan=English&cat=Meetings%2FEvents&sort=date, timestamp 2:15:00; Roy Schondorf, 'Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations', *EJIL:Talk!*, 9 December 2020, available at https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/; and New Zealand Ministry for Foreign Affairs and Trade, 'The Application of International Law to State Activity in Cyberspace', 01 December 2020, paras 16-17., on file with authors. See also Michael Schmitt, 'New Zealand Pushes the Dialogue on International Cyber Law Forward', *Just Security*, 8 December 2020, available at https://www.justsecurity.org/73742/new-zealand-pushes-the-dialogue-on-international-cyber-law-forward/.

Due diligence in international law and its applicability to ICTs

consensus has been reached about what is 'cyber due diligence' or there would be a legal gap in protection — states would have no binding obligations but only voluntary undertakings to behave diligently in their use of ICTs. The confusion partly stems from the inconsistent use of the label 'due diligence' as a general principle of law or international law, one or more state obligations, or a standard of behaviour applying in different areas of international law.[9]

To avoid those confusions and contradictions, we propose to shift the debate from label to substance. Rather than simply inquiring whether 'due diligence' applies in cyberspace, the key question we should be asking is to what extent states have obligations to protect other states and individuals from cyber harms. In answering this question, we conclude that whether or not a general principle of due diligence applies to ICTs or a binding, cyber-specific 'due diligence rule' exists, states continue to be bound by a patchwork of duties to prevent, stop and redress harm applying by default to cyberspace. These 'protective obligations' are grounded in several primary rules of international law enshrining a standard of due diligence — that is, obligations that require states to exert their best efforts in preventing, halting and redressing a variety of harms, online and offline.

This Chapter begins in Section 2 by explaining why, despite the longstanding confusion surrounding its exact meaning and scope, we believe 'due diligence' in international law is better understood as a standard of conduct. This standard usually refers to harm prevention, mitigation and redress, but it varies across the different 'protective' obligations where it is found, as well as the states, circumstances and fields in which they apply. Examples include 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.[10]

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

10 Koivurova, *supra* note 10, paras 29-31, 45.

Due diligence in international law and its applicability to ICTs

Referring back to some of the conclusions reached in Chapter 1, Section 3 then explains why the said 'protective' obligations apply 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*.

In what is this report's main contribution to the current academic debate, Section 4 maps out four sets of protective duties requiring States to prevent, halt or redress certain harms by behaving diligently in cyberspace. Two of these can be traced to primary obligations of general 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, articulated in the *Corfu Channel* case,[11] which we call the 'Corfu Channel' principle;[12] and b) states' duty to prevent and remedy significant transboundary harm, even if caused by lawful activities, known as the 'no-harm' principle.[13] 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 their jurisdiction; and d) states' duties to ensure respect for IHL 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, unpack the various standards of due diligence they enshrine and explore the extent to which they apply to States' use of ICTs.

Lastly, Section 5 demonstrates that, despite their multifaceted nature, common features belie different protective obligations. As such, they might apply concurrently and inform one another's interpretation in cyberspace and beyond.

11 *Corfu Channel Case (United Kingdom v Albania)*, Judgment, 9 April 1949, ICJ Reports (1949) 4, at 22.

12 August Reinisch and Markus 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.

13 See *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.

The 'patchwork approach' marks a paradigm shift in the understanding and conceptualisation of international law concerning diligent State behaviour in cyberspace. Though not a silver bullet against current cybersecurity challenges, we conclude that this international legal 'patchwork' of protective obligations does provide a solid and comprehensive legal basis for harm prevention and accountability.

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

Despite the renewed interest in due diligence,[14] the concept is not new. Its modern origins can be traced back to a series of nineteenth and early twentieth century arbitrations relating to the protection of aliens abroad.[15] 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 at hand, and holding them responsible for wilfully negligent omissions. Later on, the *Island of Palmas* arbitral award found that such obligation is a corollary of States' sovereign rights over their territory, requiring them to protect the rights of other States therein.[16] Since then, the concept has evolved alongside several primary rules of international law.

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*,'[17] most — but not all — of which constitute internationally wrongful acts.[18]

14 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 10; Heike Krieger, Anne Peters and Leonhard Kreuzer (eds.), *Due Diligence and Structural Change in the International Legal Order* (2020); Joanna Kulesza, *Due Diligence in International Law* (2016); Riccardo Pisillo-Mazzeschi, 'The Due Diligence Rule and the Nature of the International Responsibility of States', 35 *GYIL* (1992) 9.

15 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.

16 *Island of Palmas Case (or Miangas), United States v Netherlands, Award*, 4 April 1928, II RIAA 829 (1928), ICGJ 392 (PCA 1928), at 839.

17 Emphasis added. *Corfu Channel*, *supra* note 12, at 22.

18 See Section 4.A, below.

Due diligence in international law and its applicability to ICTs

This duty, framed as a 'well-recognized principle of international law', applies generally to all states,[19] and a failure to exercise the requisite degree of diligence gives rise to state responsibility.[20]

Second, as a result of the growing concern over environmental harm 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.[21] This obligation exists at least since 1941, when 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.'[22] Likewise, Article 3 of the International Law Commission (ILC)'s 2001 Draft Articles on Prevention of Transboundary Harm from Hazardous Activities[23] 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[24] 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,[25] which noted its origins in the broader 'principle of prevention', alongside the Corfu Channel principle.[26]

19 *Corfu Channel*, *supra* note 12, at 22.

20 See Article 14(3), United Nations International Law Commission (ILC), Articles on Responsibility of States for Internationally Wrongful Acts, GA Res. 56/83, 12 December 2000 (ARSIWA).

21 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, qt 144, 148-149. See also Jutta Brunnée and Tamar Meshel, 'Teaching an Old Law New Tricks: International Environmental Law Lessons for Cyberspace Governance', 58 GYIL (2015) 129, at 134–135; Koivurova, *supra* note 10, paras 16, 23, 44-45.

22 *Trail Smelter Case (USA v Canada)* (1941) 3 RIAA 1911, at 1963.

23 ILC, *Draft Articles on Prevention*, *supra* note 21.

24 Koivurova, *supra* note 10, para 10.

25 *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 8 July 1996, ICJ Reports (1996) 226, para 2.

26 *Pulp Mills*, *supra* note 14, para 101.

Due diligence in international law and its applicability to ICTs

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,[27] to the extent possible.[28] Likewise, the duties to ensure respect for IHL and to take precautions to protect civilians against the effects of attacks during armed conflict are also obligations to exercise due diligence.[29] 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,[30] the obligation to prevent marine pollution,[31] the duty to ensure that mining activities in the deep seabed area do not cause damage to the environment and human life,[32] and duties to cooperate in the investigation and prosecution of transnational crime.[33]

This variety of primary rules recognising a duty of reasonable care suggests that 'due diligence' itself is simply a standard of behaviour which is found in different 'protective' state obligations and varies across different fields, duty-bearers and factual circumstances.[34] Thus, references made in the literature to 'due diligence obligations' or 'duties of due diligence' seem to be a shorthand for a series of obligations which have in common the imposition of a preventive or remedial duty, compliance with which is measured against a certain standard of

27 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, para. 1.

28 See generally Koivurova, *supra* note 10, para 45.

29 Ibid., para 31.

30 Article 1, Convention on the Prevention and Punishment of the Crime of Genocide, 1948, 78 UNTS 277. See also *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.

31 Article 194(2) of the UN Convention on the Law of the Sea, 1982, 1833 UNTS 397.

32 Articles 139, 153(4) and Annex III, Article 4(4), Convention on the Law of the Sea. See also *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.

33 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.

34 See Krieger and Peters, 'Due Diligence and Structural Change in the International Legal Order', in Krieger, Peters and Kreuzer, *supra* note 14. See also McDonald, *supra* note 10.

Due diligence in international law and its applicability to ICTs

diligent behaviour.[35] Thus, lack of due diligence gives rise to a breach of an international obligation, in the same way that negligence, or lack of reasonable care, entails a breach of a duty of care in many domestic legal systems.[36] As the International Law Association (ILA) found in its recent study on the topic:

> '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.'[37]

Those various duties primarily 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.[38] It is for this reason that we conceptualise and frame them as 'protective obligations', in that they require the duty-bearer to behave diligently in protecting the beneficiary against harm. Possible sources of harm include stage agents, private individuals acting alone or in groups, as well as corporations. Beneficiaries, who may or may not hold a specific right vis-à-vis the duty-bearer, could be other states, individuals or private companies.[39] When the duty-bearer state is the very source of the harm affecting an individual or an object, and the relationship with the beneficiary is linear rather than triangular, whether or not the protective duty is one of due diligence depends on the primary

35 See Koivurova, *supra* note 10, paras 8-9.

36 Robert 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 14, at 40, 42; *Neer* case, *supra* note 15, at 61.

37 Emphasis added. *ILA Study*, *supra* note 14, at 2. See also Kulesza, *supra* note 14, at 262-270.

38 Besson, 'Due Diligence and Extraterritorial Human Rights Obligations – Mind the Gap!', 9:1 *ESIL Reflections* (2020) 2, at 4-5.

39 Ibid., at 5.

Due diligence in international law and its applicability to ICTs

obligation in question. The Corfu Channel principle seems to be limited to a duty to prevent *third-party* activities that cannot be attributed to the duty-bearer state.[40] In contrast, the no-harm principle,[41] duties to protect and ensure human rights,[42] and obligations to take precautions under IHL,[43] all seem to apply not only to cases where the duty-bearer state fails to prevent harm by third parties but also where the state *itself* causes the harm in question and thereby fails to prevent, stop or redress it.

Protective obligations have been commonly associated with the idea that states must behave diligently with a view to preventing, stopping or redressing 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.[44] However, as will become clearer in the following sections, each of those elements might differ across various protective duties.

40 Pisillo-Mazzeschi, *supra* note 14, at 31-34, citing *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)*, Judgment, 27 June 1986, ICJ Reports (1987) 14, para 157, and its finding that the United States was responsible for actively supporting the Contras, thus breaching its duty to abstain from such support, whereas Nicaragua was responsible for tolerating arms traffic thus breaching its due diligence duty to protect.

41 ILC, *Draft Articles on Prevention*, *supra* note 21, at 159, Commentary to Article 8, para 2, and at 169, Commentary to Article 11, para 1.

42 See, e.g., 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, paras 25, 28-30; ECtHR (European Court of Human Rights), Guide on Article 2 of the European Convention on Human Rights: Right to Life, Updated on 31 December 2019, para 101.

43 See, e.g., Arts 57-58 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, and International Committee of the Red Cross (ICRC), Customary IHL Database, Rule 15, available at https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule15.

44 See Section 4 below.

3. The Applicability of Existing Protective Obligations in Cyberspace

As a preliminary point, the applicability of existing protective obligations to cyberspace might be challenged on two principal 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.[45] Secondly, it could be argued that 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, we recall that a number of states and international organisations have consistently affirmed the application of international law *as a whole* to cyberspace, including, in particular, rules and principles that flow from sovereignty.[46] As argued in Chapter 1, this is because rules of general international law

45 See, *mutatis mutatis*, Gary P. Corn and Robert 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/Ir/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, para. 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.').

46 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'), para. 19; UN GGE Report 2015, *supra* note 5, paras 24-28; United States (US) Department of Defense, 'General Counsel Remarks at US Cyber Command Legal Conference, Remarks By Hon. Paul C. Ney, Jr.', 2 March 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', May 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', 23 May 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', 20 June 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 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 paras 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 27.

Due diligence in international law and its applicability to ICTs

apply, by default and across the board, to all areas and types 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 displace them.[47]

Two key 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.[48] In the same vein, the scope of application of IHRL and IHL is broad, only limited by their respective triggers and subject-matter.[49] 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.[50]

On the contrary, not only have states invoked international law, IHRL and IHL in general but also supported the applicability of different protective obligations in cyberspace, even if in a somewhat fragmented way. For instance, as far back as in 2011, the then United States (US) government recognized the application of positive IHRL duties as well as a duty to prevent cybercrime online.[51] Shortly thereafter, the Council of Europe issued a Recommendation recognizing the applicability of the no-harm principle to malicious cyber activities.[52]

47 *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, para. 120. See also Dapo Akande, Antonio Coco, Talita de Souza Dias, 'Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond', *EJIL:Talk!*, 5 January 2021, available at https://www.ejiltalk.org/old-habits-die-hard-applying-existing-international-law-in-cyberspace-and-beyond/.

48 *Tallinn Manual 2.0*, *supra* note 6, at 31, para 4; Enenu 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; Pallavi Khanna, 'State Sovereignty and Self-Defence in Cyberspace', V(4) *BRICS Law Journal* (2018) 139, at 141. See, generally, *Nuclear Weapons*, *supra* note 25, para 39.

49 *Nuclear Weapons*, *supra* note 25, paras 86.

50 ILC, *Fragmentation Report*, *supra* note 47, at para. 109.

51 US, *International Strategy for Cyberspace*, *supra* note 46, at 10.

52 Council of Europe, 'Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the 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.

Due diligence in international law and its applicability to ICTs

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.[53]

Along with the abovementioned statement by the EU representative in the context of the COVID-19 crisis — which was expressly supported by Turkey, North Macedonia, Montenegro, Serbia, Albania, Bosnia and Herzegovina, Iceland, Liechtenstein, Norway, Ukraine, Moldova and Armenia[54] — several states have recently recognised slightly different iterations of due diligence in their use of ICTs, as a matter of international law. 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 cyberspace by non-state actors situated in the territory or under the jurisdiction of the State in question.'[55] 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*.[56]

53 '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, available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805ccaeb, para. 80 and more extensively paras 71-84. 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', available at http://humanrightseurope.blogspot.com/2011/01/proposals-for-international-cooperation.html, paras 59-74 and in particular paras 72-74 on the standard of due diligence.

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

55 Emphasis added. 'Statement by France's Deputy Permanent Representative at the UN at the UNSC Arria-Formula Meeting on Cybersecurity, Ms. Anne Gueguen', 22 May 2020, available at https://youtu.be/K704P5D1n3E (timestamp 25:00). See also France, *Droit International Appliqué*, *supra* note 46, 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.

56 Emphasis added. Estonia, 'President of the Republic at the opening of CyCon 2019', 29 May 2019, available at https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html.

Due diligence in international law and its applicability to ICTs

Using 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'.[57] 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*, whether using ICTs or otherwise'.[58] 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'.[59] And, in what seems to combine different rules, 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*.[60]

Similar statements have been made by the Czech Republic,[61] the Republic of Korea,[62] Austria,[63] the Dominican Republic,[64] Chile,

57 Emphasis added. *Australia's Non Paper*, *supra* note 46, 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.

58 Finland, '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, February 10 and 11', February 2020, available at https://ccdcoe.org/uploads/2018/10/Statement-on-International-Law-by-Finnish-Ambassador-Janne-Taalas-at-2nd-session-of-OEWG.pdf.

59 Ibid.

60 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', 5 July 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.

61 Czech Republic, *supra* note 46, at 3.

62 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.

63 Austria, *supra* note 46, at 2-5.

64 '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.

Due diligence in international law and its applicability to ICTs

Ecuador, Guatemala, Guyana and Peru.[65] These provide further support to the view that *existing* protective obligations containing a due diligence standard are fully applicable to ICTs, even if their specific implementation requires additional guidance. Taken together, they overshadow the contrary statements made so far by Argentina, Israel and New Zealand, which, as noted in Chapter 1, either reject or question the applicability of due diligence duties to ICTs.[66]

That said, two important questions remain open: a) whether an all-encompassing 'principle of due diligence' exists *generally* in international law; and b) whether a single protective obligation — with a corresponding due diligence standard — exists *specifically* for cyberspace.[67] In particular, some have suggested that Rule 6 of the Tallinn Manual 2.0 and similar cyber-articulations of the concept of due diligence are *lex ferenda*[68] or simply proposed interpretations of how an existing, wide-ranging 'due diligence obligation' should apply to ICTs.[69] They have pointed to several reasons of policy behind states' reluctance to commit to a new, cyber-specific rule. For instance, states may fear that a fine-grained due diligence standard for ICTs would be too burdensome to implement and could stifle its necessary flexibility.[70] Alternatively, such a new obligation may put in question the applicability and binding character of existing ones.[71] It is also possible that, by widening the scope of unlawful acts in the ICT

65 OAS, *Improving Transparency*, *supra* note 45, para. 58. See also paras 56ff.

66 *Supra* note 8.

67 See, e.g., The Netherlands, *Letter of 5 July 2019 (Appendix)*, *supra* note 60, 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.'

68 See Michael 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 *Tallinn Manual 2.0*, *supra* note 6, at 32, para 6; US, *International Strategy for Cyberspace*, *supra* note 46, at 10 (listing 'Cybersecurity Due Diligence' as an emerging norm specific to cyberspace); Argentina, *supra* note 8.

69 See, e.g., Marko Milanovic and Michael Schmitt, 'Cyber Attacks and Cyber (Mis)information Operations during a Pandemic', 11 *Journal of National Security Law & Policy* (2020) 247, at 280 (arguing, that '[t]his obligation is simply the cyber application of a *wide-ranging* due diligence positive obligation under general international law requiring a state to stop harm to the rights of other states emanating from its territory', emphasis added); France, *Response to the OEWG pre-draft report*, *supra* note 55, at 1-2; Czech Republic, *supra* note 46, at 3.

70 Jensen and Watts, *supra* note 8, at 1574; Adamson, *supra* note 8, at 55, para. 12.

71 Austria, *supra* note 46, 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.

environment, a new protective 'cyber due diligence' obligation could increase resort to countermeasures and litigiousness among states.[72]

Perhaps the choice of using 'due diligence' to label a range of duties is misleading: its simplicity masks the complexity and diversity of protective obligations requiring diligent behaviour to prevent, halt and redress certain harms. Part of the confusion also seems to arise from the framing of ICTs as a new space or 'domain', rather than a new set of information and communication technologies or tools.[73] Nevertheless, the important takeaway is this: 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' already requires States to behave diligently in preventing, halting and redressing different types of harmful cyber operations.

4. The Patchwork of International Obligations to Prevent, Halt and Redress Cyber Harms

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-

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

73 See Akande, Coco and de Souza Dias, *supra* note 47.

74 See *supra* notes 52-65.

75 See, e.g., *Tallinn Manual 2.0*, *supra* note 6, at 35-36, para 21; Milanovic and Schmitt, *supra* note 69, 280; Michael Schmitt, 'In Defense of Due Diligence in Cyberspace', 125 *The Yale Law Journal Forum* (2015) 68; Karine 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; Joanna Kulesza, 'Due Diligence in International Internet Law', *Journal of Internet Law* (2014) 24, at 27-28; Robin Geiss and Henning Lahmann, 'Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention', in Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy* (NATO CCD COE Publication, 2013) 621, at 635; Oren Gross, 'Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents', 48 *Cornell International Law Journal* (2015) 481, at 494; Martin Ney and Andreas Zimmermann, 'Cyber-Security Beyond the Military Perspective: International Law,

Due diligence in international law and its applicability to ICTs

recognized' Corfu Channel principle, requiring a state '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] 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 the 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.

'Cyberspace', and the Concept of Due Diligence', 58 *GYIL* (2015) 51, at 61-62; Christian Walter, 'Obligations of States Before, During, and After a Cyber Security Incident', 58 *GYIL* (2015), 67, at 73-76; Oliver 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 12, at 22 (emphasis added).

77 *Island of Palmas*, *supra* note 2, at 839. See also, *Australia's Non Paper*, *supra* note 46, 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.

80 *Corfu Channel*, *supra* note 12, at 18. On the requirement of knowledge as applied to cyberspace, see *Tallinn Manual 2.0*, *supra* note 6, pages 40-41.

81 Nicaragua, *supra* note 40, 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 Constantine Antonopoulos, 'State responsibility in cyberspace', in Nicholas Tsagourias and Russell Buchan (eds), *Research handbook on international law and cyberspace* (Edward Elgar, 2015) 55, at 69.

83 *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 55, at 3; and The Netherlands, *Letter of 5 July 2019 (Appendix)*, *supra* note 60, at 4.

Due diligence in international law and its applicability to ICTs

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 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, which may or may not constitute an unlawful act, 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

85 *Tallinn Manual 2.0*, *supra* note 6, at 34, 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 60, at 4; Okwori, *supra* note 48, at 219-220; Barrie 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 69, at 280.

86 *Tallinn Manual 2.0*, *supra* note 6, at 35-36, para 21.

87 See *Affaire des biens britanniques au Maroc espagnol*, *supra* note 78, at 643-644; Koivurova, *supra* note 10, para 2; Dörr, *supra* note 75, at 90; Kolb, *supra* note 36, at 119.

88 *Tallinn Manual 2.0*, *supra* note 6, at 35-36, paras 18-22.

Due diligence in international law and its applicability to ICTs

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 remotely conducted 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 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 victim 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

89 Article 27, ARSIWA.

90 See below, Section 4(A)(ii).

91 'Press release: UK condemns cyber actors seeking to benefit from global coronavirus pandemic', 5 May 2020, available at https://www.gov.uk/government/news/uk-condemns-cyber-actors-seeking-to-benefit-from-global-coronavirus-pandemic.

92 Kolb, *supra* note 36, at 121; The Netherlands, *Letter of 5 July 2019 (Appendix)*, *supra* note 60, at 5.

93 See *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 48, at 218-219. See also *The Netherlands, Letter of 5 July 2019 (Appendix)*,

Due diligence in international law and its applicability to ICTs

articulations 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 ICTs.[97]

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 even corruption of data may not, according to some ,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

supra note 60, 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 68, at 54.

96 See, e.g., Irène 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 48, at 208-213; Geiss and Lahmann, *supra* note 75, 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; Brunnée and Meshel, *supra* note 21, at 133-135; Jensen and Watts, *supra* note 8, at 1565-1566.

97 *Tallinn Manual 2.0*, *supra* note 6, at 30-32, paras 1-5. See also Milanovic and Schmitt, *supra* note 69, at 280.

98 Beatrice Walton, 'Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law', *Yale Law Journal* (2016) 1460, at 1466, 1475-1477; Rebecca 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 45, at 209-210. But see *Tallinn Manual 2.0*, *supra* note 6, at 18-22 and 171 (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 or if they interfere with or usurp the inherently governmental functions of a state, even if conducted remotely). See also Russell Buchan, *Cyber Espionage and International Law* (2019), at 51.

100 *Tallinn Manual 2.0*, *supra* note 6, at 36, para 23.

Corfu Channel principle does is not limited to transboundary acts.[101]

As mentioned in Chapter 3, debates continue as to whether sovereignty is a separate rule of international law which is applicable to ICTs. However, we believe that the better view is that, if sovereignty or territorial sovereignty can be breached generally, then there is no reason to deny that breaches of sovereignty may occur in states' use of ICTs.[102] If that is so, then the scope of acts contrary to the rights of other states to sovereignty or territorial sovereignty over ICTs would be potentially large, including cyber operations that produce physical or functional damage on the territory of the victim state or which undermine its inherently governmental functions.[103] And because there is no need for such acts to amount to an internationally wrongful act attributable to a state, they may well be perpetrated by non-state actors, in which case the origin or transit state may be held responsible for failing to prevent or halt the activity in question. In assessing whether a state's right to sovereignty has been contravened, relevant factors include the scope, scale, impact or severity of the disruption caused, including how many states, legal and natural persons were affected, the amount of economic loss caused and the amount or nature of compromised data.[104]

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.[105] For the Experts, the Corfu Channel principle only applies

101 This position seems to have been implicitly endorsed in *Tallinn Manual 2.0*, *supra* note 6, at 39, para 32.

102 Similarly, but limited to *territorial* sovereignty, see Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention* (Chatham House, 2020), paras 40-50.

103 *Tallinn Manual 2.0*, *supra* note 6, at 19-27, Rule 4, paras 10-32.

104 Moynihan, *supra* note 102, paras 67-70 citing, *inter alia*, EU Council, 'Council decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States', (CFSP) 7299/19, 14 May 2019, available at https://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf, Art 3.

105 *Tallinn Manual 2.0*, *supra* note 6, at 31, para 5; at 41-42, para 42, at 44-45, paras 7, 10.

Due diligence in international law and its applicability to ICTs

to *ongoing* or at most *imminent* operations, at least as far as cyberspace is concerned.[106] This would limit the scope of the duty to an obligation to simply halt harmful cyber operations.[107] As a consequence, when discharging this duty, states would not be required to adopt strictly preventive, *ex ante* measures such as continuous supervision or monitoring of their networks.[108]

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.[109] However, 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.[110] 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 a separate obligation to put in place the minimum governmental infrastructure that is reasonable in the circumstances, enabling a State to exercise the necessary degree of diligence.[111] In this sense, two limbs make up the Corfu Channel

106 Ibid., at 43-44, paras 3-4. See also Okwori, *supra* note 48, at 216.

107 *Tallinn Manual 2.0*, *supra* note 6, at 44-45, para 7.

108 Ibid., at 44-45, paras 7 and 10; Couzigou, *supra* note 96, at 50-51; Okwori, *supra* note 48, at 215; Jensen and Watts, *supra* note 8, at 1566; Akiko Takano, 'Due Diligence Obligations and Transboundary Environmental Harm: Cybersecurity Applications', 36 *Laws* (2018) 7, at 8. See also *ILA Study*, *supra* note 14, at 7-8; Estonia, *supra* note 56; *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.

109 *Tallinn Manual 2.0*, *supra* note 6, at 45, para 8. See also Okwori, *supra* note 48, at 215; Crootof, *supra* note 98, at 611, Jack 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.

110 *Tallinn Manual 2.0*, *supra* note 6, at 47, para 16-18; Buchan, *The Obligation to Prevent*, *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 108, at 2; The Netherlands, *Letter of 5 July 2019 (Appendix)*, *supra* note 60, at 5; *Australia's Non Paper*, *supra* note 46, at 8; *New Canadian text proposals*, *supra* note 94, at 3. On obligations of transit states, see *Tallinn Manual 2.0*, *supra* note 6, at 33-34, para 34.

111 See Buchan, *The Obligation to Prevent*, *supra* note 1, at 436-437; Kolb, *supra* note 36, at 127, Couzigou, *supra* note 96, at 50-51; Takano, *supra* note 108, at 9.

Due diligence in international law and its applicability to ICTs

principle, as well as other rules incorporating a due diligence standard.[112]

First, there is an obligation to set up a minimal state apparatus — a core 'capacity-building' duty. This is likely an obligation of result, i.e., a baseline governmental infrastructure *must* be established.[113] If a state could simply claim that it has exercised its best efforts for this purpose, the main duty to prevent, halt and redress harm could be easily evaded. Yet the content of such capacity-building duty – the result required from each state – should not be fixed, but dependent on the circumstances at hand, particularly available human and financial resources.

Second, there is an obligation *of conduct* to exercise due diligence, 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. 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.[114] While this may raise concerns about privacy and other rights, for present purposes, 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.[115]

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

112 Pisillo-Mazzeschi, *supra* note 14, at 26-27; ILC, *Draft Articles on Prevention*, *supra* note 21, at 155, Commentary to Article 3, paras 15-17.

113 Pisillo-Mazzeschi, *supra* note 14, at 26; Buchan, *The Obligation to Prevent*, *supra* note 1, at 434-439.

114 See *supra* note 108.

115 See Bannelier-Christakis, *supra* note 75, at 31; Dörr, *supra* note 75, at 95.

Due diligence in international law and its applicability to ICTs

known about a serious risk that a cyber operation contrary to the rights of other states will take place, no matter how remote such risk is.[116] As the Tallinn Manual itself acknowledges, it is the actual or constructive knowledge of *a serious risk* that triggers said obligation.[117] 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.[118] The same applies to transit states, to the extent that they have actual or constructive knowledge of the risk of a cyber operation contrary to the rights of other states, as well as the capacity to prevent it.[119] 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 through their territory which would be contrary to the rights of other States.[120] What it does require is the minimum governmental infrastructure or capacity enabling states to *acquire* such knowledge.[121]

In short, 'the more states *can* do, the more they must do',[122] and great responsibility follows inseparably from great power,[123] 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

116 See Kolb, *supra* note 36, at 123-124.

117 *Tallinn Manual 2.0*, *supra* note 6, at 45, para 9 and Ibid., at 44-45, para 7, citing *Bosnian Genocide Case*, *supra* note 82, para 431.

118 See, *mutatis mutandi*, *Bosnian Genocide Case*, *supra* note 82, para 436.

119 Similarly, Couzigou, *supra* note 96, at 43, 47; Buchan, *The Obligation to Prevent*, *supra* note 1, at 441. See *contra* Reinisch and Beham, *supra* note 12, at 106-107; Okwori, *supra* note 48, at 226-227.

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

121 See *supra* note 111.

122 John Heieck, Symposium: A Duty to Prevent Genocide–Due Diligence Obligations among the P5 (Part One), *Opinio Juris*, 10 December 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).

123 *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).

possible.[124] In many circumstances, reporting and sharing information about incidents will suffice.[125]

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.[126] There are at least four significant differences between these 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.

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 'significant transboundary harm' or the risk thereof, even if caused by lawful activities and even if no state right is contravened.[127] Yet two sets of questions have often been raised with regards to the applicability of this principle in the context of states' use of ICTs. The first is whether the no-harm principle applies beyond the environmental realm to cover 'non-ecological' harm. The second, broader, question is, even if the principle extends beyond the natural environment, whether it covers non-physical harm, such as financial losses or reputational damage.

124 Similarly, Kolb, *supra* note 36, at 123.

125 Gross, *supra* note 75, at 506.

126 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 98, at 1486-1487; Sander, *supra* note 85, at 49.

127 ILC, *Draft Articles on Prevention*, *supra* note 21, at 150, Commentary to Article 1, para 6; 152, Commentary to Article 2, para 5. See also Koivurova, *supra* note 10, para 11; Crootof, *supra* note 98, a 600.

Due diligence in international law and its applicability to ICTs

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'.[128] And for the avoidance of any doubt, the ILC Special Rapporteur on the topic, Richard Quentin-Baxter, clarified that the scope of the Articles 'will include all physical uses of territory giving rise to adverse physical transboundary effects'.[129] In particular, he noted that:

> 'No short phrase exactly describes the full extent of this field of application, and some doubts have been raised by an injudicious reliance upon references to "environment" or "physical environment". A warning about this source of ambiguity was given during the Commission's discussions at its thirty-second session, in 1980, and a similar question arose during the consideration of the Commission's report in the Sixth Committee of the General Assembly, at its thirty-seventh session, in 1982. It should therefore be confirmed that there was never an intention to propose a reduction in the scope of the topic to questions of an ecological nature, or to any other subcategory of activities involving the physical uses of territory; nor, indeed, did any speaker in the Sixth Committee urge the desirability of such a reduction'.[130]

Looking further back at the history of the principle, 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.[131] 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.[132] Similarly, according to the ICJ, the no-harm principle is a manifestation of the general principle of

128 ILC, *Draft Articles on Prevention*, *supra* note 21, at 152-153, Article 2(b) and Commentary, paras 8 and 9.

129 '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 ('*Fourth report on international liability*'), 27 June 1983, para 17.

130 Ibid.

131 *Trail Smelter*, *supra* note 22, at 1963.

132 Ibid., at 1963-1965.

Due diligence in international law and its applicability to ICTs

prevention and therefore closely related to the Corfu Channel rule.[133] Granted, this general finding was made in the context of a state's obligation 'to use all the means at its disposal in order to avoid activities which take place in its territory, or in any area under its jurisdiction, causing significant damage to the environment of another State'.[134] Yet, that the Court specifically highlighted the existence of this duty, 'now part of the corpus of international law relating to the environment',[135] as was relevant to the case at hand, by no means exhausts or negates the *general* applicability of the no-harm principle and other principles of prevention, beyond the environmental realm.

Finding an answer to the second question outlined earlier, i.e., whether the no-harm principle applies to non-physical harm, may be more difficult. Nonetheless, there is significant evidence that it does. First, it is worth noting that the ILC's decision to focus its Draft Articles on the prevention of *physical* harm and 'exclude transboundary harm which may be caused by State policies in monetary, socio-economic or similar fields' was made 'in order to bring this topic within a manageable scope'[136] and given 'that State practice [was then, in 1983] insufficiently developed in other areas'.[137] Specifically, the Special Rapporteur noted that there was 'no sufficiently broad agreement at the international level about the distinctions—well developed in municipal legal systems—between fair and unfair competition'.[138]

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 that informed the Commission's work on the prevention

133 *Pulp Mills*, *supra* note 14, para 101.

134 Ibid.

135 Ibid., citing *Nuclear Weapons*, *supra* note 25, para 29.

136 ILC, *Draft Articles on Prevention*, *supra* note 21, at 151, Commentary to Article 1, para 16.

137 *Fourth report on international liability*, *supra* note 129, para 63.

138 Ibid, para 14 (see also paras 12-13 and 63).

Due diligence in international law and its applicability to ICTs

of transboundary harm.[139] Examples of non-material injuries that have given rise to claims of liability for transboundary harm include lost revenues or future interests resulting from territorial delimitation,[140] 'anxiety' arising from potential nuclear damage,[141] and population relocation costs.[142] Tellingly, in its very first survey of state practice, conducted in 1984, the ILC found that:

> Injury, for purposes of prior negotiation and consultation, may be subdivided into material, non-material and potential. There is no intention here clearly to define injury or harm. For the purposes of this study, material harm means "physical", "quantitative" or "tangible" injury to a State's interests. Non-material harm refers to 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 inconsistent with its internal order and its territorial integrity.[143]

Evidence of state practice substantiating this finding notably include: 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;[144] 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

139 ILC, 'Liability regimes relevant to the topic "International liability for injurious consequences arising out of acts not prohibited by international law": survey prepared by the Secretariat', UN Doc A/CN.4/471 23 June 1995 ('*1995 Survey of liability regimes*'), paras 253-271; Survey of liability regimes relevant to the topic of international liability for injurious consequences arising out of acts not prohibited by international law (international liability in case of loss from transboundary harm arising out of hazardous activities), prepared by the Secretariat, UN Doc A/CN.4/543, 24 June 2004 ('2004 *Survey of liability regimes*'), paras 526-530.

140 Survey of State practice relevant to international liability for injurious consequences arising out of acts not prohibited by international law, prepared by the Secretariat, UN Doc A/CN.4/384, 16 October 1984 ('*1984 Survey of liability regimes*'), para 165, citing Separate Opinion of Judge Jessup, *North Sea Continental Shelf (Germany v Denmark and the Netherlands)*, Judgement (1969) ICJ Rep 3.

141 *2004 Survey of liability regimes*, *supra* note 139, para 520.

142 *1995 Survey of liability regimes*, *supra* note 139, para 259.

143 *1984 Survey of liability regimes*, *supra* note 140, para 115.

144 Ibid, para 58.

Due diligence in international law and its applicability to ICTs

parties, or of private enterprises recognised or authorised by them to conduct a radiocommunication service;[145] 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.[146]

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.[147] If since 1927, states have consistently recognised duties to prevent remote harm to or interference with other states' ICTs of the day, one would reasonably expect that the harm caused by 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. As the ILC Special Rapporteur on international liability noted, the duty to prevent transboundary harm 'is a concomitant of the exclusive or dominant jurisdiction which international law reposes in the source State as a territorial or controlling authority.'[148] Thus, if states exercise their sovereign powers over ICTs within or outside their territory, they ought to have the concomitant duty to prevent their use from harming other states.

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.'[149] This could mean that, if there is a foreseeable risk (ILC, Draft articles on Prevention, Commentary to Article 3, para 5) that the use of ICTs may lead to significant transboundary harm, such as the exploitation of another state's critical systems, such as electric and nuclear

145 Ibid, para 59.

146 Ibid.

147 Constitution and Convention of the International Telecommunication Union (with annexes and optional protocol), adopted on 22 December 1992, entered into force 1 July 1994, 1825 UNTS 31251.

148 *Fourth report on international liability*, *supra* note 129, para 63.

149 ILC, *Draft Articles on Prevention*, *supra* note 21, at 155, Commentary to Article 3, para 18.

Due diligence in international law and its applicability to ICTs

power plants, or health and life-saving equipment in hospitals, then greater diligence is required from the state from which the operation originated. [150]

Thus, there are strong reasons to suggest that it covers *any* type of transboundary harm,[151] including harms committed through ICTs, whether or not they are contrary to the rights of other states.[152] Admittedly, many harmful cyber operations *will* be contrary to at least one rule of international law and will likely be contrary to the rights of other states. 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 breach such rule.[153] Likewise, coercive interferences with a state's core governmental functions, such as its electoral processes, would violate the principle of non-intervention.[154] 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.[155] This should be true at least for *negative* human rights obligations,[156] for which a state's jurisdiction may be triggered by the exercise of control over the activity in question,[157] the ICT infrastructure used[158] or the enjoyment

150 Ibid, at 153-154, Commentary to Article 3, paras 5 and 11.

151 See *supra* note 21 and Crootof, *supra* note 98, at 603-604; Walton, *supra* note 98, at 1465, 1479-1481; Sander, *supra* note 85, at 51.

152 See, e.g., Crootof, *supra* note 98, at 603-604; Walton, *supra* note 98, at 1480-1482, 1497; Sander, *supra* note 85, a 49-50; Reinisch and Beham, *supra* note 12, at 104-106; Dörr, *supra* note 75, at 93; Buchan, *The Obligation to Prevent*, *supra* note 1, at 439-452; Okwori, *supra* note 48, at 210; Takano, *supra* note 108. See also *Interim Report of the Ad-hoc Advisory Group on Cross-border Internet*, *supra* note 53, paras 60-65.

153 *Tallinn Manual 2.0*, *supra* note 6, at 17-20, esp. para 7; Michael Schmitt and Liis Vihul, 'Respect for Sovereignty in Cyberspace', 95 *Texas Law Review* (2017) 1639, at 1648-1649.

154 See, e.g., Sean Watts, 'Low-Intensity Cyber Operations and the Principle of Non-Intervention', in Jens D. Ohlin *et al.* (eds), *Cyber War: Law and Ethics for Virtual Conflicts* (Oxford University Press, 2015) 250, at 257. But see Sander, *supra* note 85, at 20.

155 Sander, *supra* note 85, at 35-43.

156 See Marko Milanovic, *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy* (Oxford University Press, 2011), at 209; Sander, *supra* note 85, at 39-43. On extraterritorial jurisdiction over online harms, see Section C(i) *infra*.

157 *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, para. 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.

158 '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, para. 34.

of the victim's human rights,[159] 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.[160] This gives the principle a potentially wide scope of application which is particularly well-suited for ICTs, where debates continue as to the nature of sovereignty, jurisdiction and prohibited intervention, as seen in Chapter 3.[161] 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.[162] Although the principle requires the crossing of an international boundary,[163] it is not limited to physical harms.[164] Often referred to as 'international cybertorts',[165] these transboundary operations may include substantial financial loss, functional and/or physical damage to networks or systems, data corruption or loss, reputational or political damage.[166]

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:

159 HRC, *General Comment 36* (*supra* n 42), para. 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.

160 Walton, *supra* note 98, at 1486. See also Finland, *Statement by Ambassador Janne Taalas*, *supra* note 61, at 2.

161 Crootof, *supra* note 98, at 592-593; Sander, *supra* note 85, at 18-24, 52.

162 Walton, *supra* note 98, at 1497-1499, 1512.

163 ILC, *Draft Articles on Prevention*, *supra* note 21, at 152-153, Article 3(c)-(e) and Commentary, paras 9-12.

164 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 22, at 1926-1927; *Nuclear Weapons*, *supra* note 25, paras 29 and 36. See also Crootof, *supra* note 98, at 603; Walton, *supra* note 98, at 1482; Buchan, *The Obligation to Prevent*, *supra* note 1, at 449-450; Takano, *supra* note 108, at 1.

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

166 Crootof, *supra* note 98, at 608-609; Gross, *supra* note 75, at 484; Takano, *supra* note 108, 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.

Due diligence in international law and its applicability to ICTs

> 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.[167]

'Significant harm', in this context, encompasses 'the combined effect of the probability of occurrence of an accident and the magnitude of its injurious impact'.[168] 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'.[169] In the context of ICTs, this could potentially include online mis- and disinformation campaigns, especially those taking place during elections[170] or public health crises.[171] The determination of what amounts to significant harm involves a somewhat subjective or value-based 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.[172] At the same time, this assessment must be based on objective or factual criteria, such as the scale and nature of the harm and its impact on different victims.[173]

167 ILC, *Draft Articles on Prevention*, *supra* note 21, at 152, Commentary to Article 2, para 4 (emphasis in the original).

168 Ibid., para 2.

169 Ibid., para 3.

170 See Sander, *supra* note 85, at 49-50.

171 See Milanovic and Schmitt, *supra* note 69. See also Olga Robinson and Marianna Spring, 'Coronavirus: How bad information goes viral', *BBC News*, 19 March 2020, available at https://www.bbc.co.uk/news/blogs-trending-51931394; Jennifer Rankin, 'Russian media 'spreading Covid-19 disinformation', *The Guardian*, 18 March 2020, available at https://www.theguardian.com/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, para. 34. On due diligence obligations applying in relation to COVID-19, see Antonio Coco and Talita de Souza Dias, 'Prevent, Respond, Cooperate: States' Due Diligence Duties vis-à-vis the Covid-19 Pandemic', *Journal of Humanitarian Legal Studies* (2020).

172 ILC, *Draft Articles on Prevention*, *supra* note 21, at 153, Commentary to Article 2, para 7.

173 Ibid at 152-153, Commentary to Article 2, paras 4 and 7.

Due diligence in international law and its applicability to ICTs

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.[174] However, the no-harm principle also covers remote risks of 'disastrous harm'.[175] This seems to imply a requirement to undertake more proactive measures of vigilance or monitoring,[176] variable on the basis of the gravity of the harm.[177] Again, a requirement for states to be continuously vigilant in their use of ICTs[178] — or any other technology for that matter — depends on its technical and economic feasibility for the state in question[179] and its compatibility with other international obligations, especially international human rights law. 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. However, a breach of the principle only occurs when the harm in question materialises. It is at this point that the responsibility of the duty-bearer is engaged, and other 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. Here, state responsibility is delayed: a breach of the no-

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

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

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

177 Ibid., at 154-155, Commentary to Article 3, paras 11 and 18; *ILA Study*, *supra* note 14, at 12; *Seabed Mining*, *supra* note 32, para 117; Koivurova, *supra* note 10, para 17.

178 In defence of a duty to continuously monitor cyberspace, see Geiss and Lahmann, *supra* note 75, at 254-255, citing *Pulp Mills*, *supra* note 14, para. 197; Buchan, *The Obligation to Prevent*, *supra* note 1, at 441-442; Bannelier-Christakis, *supra* note 75, at 30-31; Takano, *supra* note 108, at 7-8.

179 See Buchan, *The Obligation to Prevent*, *supra* note 1, at 441; Gross, *supra* note 75, at 503.

Due diligence in international law and its applicability to ICTs

harm principle arises after a state fails to compensate the victim for the damage caused.[180]

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.[181] Those consequences are, first and foremost, *liability* for the harm caused, and, second, *responsibility* for the eventual failure to redress it.[182] 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,[183] but the failure to *redress* it. The advantages of applying this regime to ICTs include increasing the costs of harmful cyber operations and deterring them, avoiding the stigma and antagonism associated with unlawful acts and fostering victim redress.[184]

180 See Crootof, *supra* note 98, at 603; Walton, *supra* note 98, at 1487-1488; Sander, *supra* note 85, at 51; Dörr, *supra* note 75, at 96.

181 Walton, *supra* note 98, at 1486-1487; Sander, *supra* note 85, at 50.

182 ILC, *Draft Articles on Prevention*, *supra* note 21, at 148, General Commentary, para 1; at 150, Commentary to Article 1, para 6. See also Walton, *supra* note 98, at 1486-1488; Sander, *supra* note 85, at 51.

183 See ILC, *Draft Articles on Prevention*, *supra* note 21, at 154, Commentary to Article 3, para 7.

184 Crootof, *supra* note 98, at 597-599, 604-608, 614; Walton, *supra* note 98, at 1511-1516.

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 fake news or censorship. Cyber-bulling, defamation and hate speech can spread incredibly quickly, with detrimental effects on individuals' rights and reputation.[185]

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.[186] In the ICT environment 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.[187] In addition, States must *ensure* the effective enjoyment of human rights on the Internet.[188] Positive obligations to protect and ensure may be potentially identified for all human rights.[189] With specific

185 ECtHR, *Delfi v Estonia*, Appl. no. 64569/09, Judgment of 16 June 2015, para 110.

186 UN GGE Report 2015, *supra* note 5, para. 28(b).

187 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 69, at 270ff.

188 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, para. 8. See also CESCR, 'General Comment No. 3: The Nature of States Parties' Obligations (Art. 2, Para. 1, of the Covenant)', E/1991/23, 14 December 1990, para. 1; IACtHR, *Velasquez Rodriguez v. Honduras*, Judgment (Merits), 29 July 1988, paras 166–167.

189 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).

Due diligence in international law and its applicability to ICTs

reference to the rights which are more commonly endangered online, one may highlight the rights to privacy,[190] honour and reputation,[191] and freedom of information and expression.[192] Due diligence, in this context, designates the standard of conduct which states are required to exercise to comply with the said positive obligations.[193]

Unlike the Corfu Channel and no-harm principles, IHRL due diligence duties are owed not only to other states, but also individuals, irrespective of nationality, and the international community as a whole. However, similarities also exist among those protective duties: positive obligations to protect human rights require states to prevent threats to the enjoyment of those right, halt harms as soon as they begin and, to the extent possible, mitigate their effects once they occur.[194] 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.[195]

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

190 ECtHR, *X and Y v. the Netherlands*, Appl. no. 8978/80, Judgement of 26 March 1985, para 23; *Bărbulescu*, *supra* note 187, 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, para. 10.

191 HRC, *General Comment 16*, *supra* note 190, paras 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.

192 HRC, 'General comment No. 34, Article 19: Freedoms of opinion and expression', UN Doc CCPR/C/GC/34, 12 September 2011, paras 12, 15.

193 HRC, *General Comment 31*, *supra* note 188, para. 8; Besson, *supra* note 38, at 2, 4-5; Schmitt and Milanovic, *supra* note 69, at 270ff.

194 With respect to civil and political rights, see HRC, *General Comment 31*, *supra* note 188, paras 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, para. 14.

195 Anja 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; Helen Keller and Retho 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 188, para. 8.

Due diligence in international law and its applicability to ICTs

mitigating the human rights impact of their activities.[196] That being said, states themselves may have a protective duty or 'due diligence' obligation to establish a legal framework that requires businesses to, in turn, exercise their own due diligence.[197]

While states' positive duties under IHRL are also subject to a requirement of capacity to act, common to other due diligence obligations,[198] they may be 'substantively … more demanding' than those deriving from general international law, often including duties to actively seek knowledge of violations.[199] In particular, for some human rights, such as the right to life, there is a separate procedural obligation of result to put in place accessible and effective measures of vindication, including the duty to take appropriate measures to investigate, prosecute, punish and remedy violations.[200] 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.[201] In IHRL, the concept of

196 On this principle, see Jonathan Bonnitcha and Robert 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 John G. Ruggie and John F. Sherman III, '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.

197 CESCR, *General Comment 24*, *supra* note 194, paras 16-18, with respect to economic, social and cultural rights — but with a principle that could be extended to civil and political rights as well; Besson, *supra* note 38, at 8.

198 Besson, *supra* note 38, at 5-7.

199 Milanovic and Schmitt, *supra* note 71, at 281-282, citing as an example CESCR, *General Comment 24*, *supra* note 194, para. 33.

200 HRC, *General Comment 36*, *supra* note 42, para 67; ECtHR, *McCann and Others v. United Kingdom*, Appl. no. 19009/04, Judgment of 27 September 1995, para 161; ECtHR, *Güzelyurtlu and Others v. Turkey*, Application no. 36925/07, Judgement of 29 January 2019, para 189.

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

Due diligence in international law and its applicability to ICTs

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,[202] extraterritorial models of jurisdiction are particularly relevant in the context of states' duties to prevent, halt and redress online harms. Five such models can be identified.

First, there is broad agreement that extraterritorial jurisdiction 'follows' individuals wherever a State exercises some form of physical control or authority over them.[203] 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.[204] As is well-known, control over individuals may be exercised through the activities of State agents abroad.[205]

Second, although not without contestation,[206] 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.[207] As such, a state's positive duties

202 Sullivan, *supra* note 3, at 454, fn 88.

203 HRC, *General Comment 31*, *supra* note 188, para 10.

204 M. Milanovic, *Extraterritorial Application*, *supra* note 156, 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.

205 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 204, paras 136-139.

206 See Besson, *supra* note 38.

207 HRC, *General Comment 36*, *supra* note 42, para. 22, with respect to the right to life; CESCR, *General Comment 14*, *supra* note 171, para. 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, para. 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, 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, *supra* note 69, at 264-265.

Due diligence in international law and its applicability to ICTs

concern the rights that may be infringed by said private entities.[208]

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.[209] While this functional approach to jurisdiction[210] has had some acceptance with respect to negative human rights duties,[211] 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.[212] 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.[213] Capacity, in this context, includes the ability to influence the behaviour of the perpetrators,[214] the unpredictability of certain events, the availability of resources, and the duty to respect and protect other human rights.[215] Of course, there is a difference between a state having no jurisdiction (and thus no human rights obligations in the first place) at all and it being incapable to protect human rights within its jurisdiction: in the latter situation, a state may still be found

208 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 38, at 2.

209 HRC, *General Comment 36*, *supra* note 42, para. 63.

210 See Shany, 'Taking Universality Seriously: A Functional Approach to Extraterritoriality in International Human Rights Law', 7 *The Law & Ethics of Human Rights* (2013) 47.

211 Milanovic, *Extraterritorial Application*, *supra* note 156, at 209; Ryan Goodman, Christof Heyns and Yuval Shany, 'Human Rights, Deprivation of Life and National Security: Q&A with Christof Heyns and Yuval Shany on General Comment 36', *JustSecurity*, 4 February 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*, *supra* note 157, para. 12.3; *Liliaan Celiberti de Casariego v Uruguay*, *supra* note 157, para. 10.3; *Issa and others v. Turkey*, *supra* note 159, para. 71.

212 See, e.g., the account of the debate in Milanovic, *The Murder of Jamal Khashoggi*, *supra* note 204, at 19-20; and Milanovic, *Extraterritorial Application*, *supra* note 156, at 209, 210-212, 219-220.

213 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.

214 *Bosnian Genocide*, *supra* note 82, para 430.

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

Due diligence in international law and its applicability to ICTs

in breach of its human rights obligations, but only insofar as it has the capacity to act. States are not required to do the impossible or to discharge a '*disproportionate burden*',[216] but are expected to adopt measures that are available and reasonable in the circumstances.[217] 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.[218]

Fourth and finally, the ECtHR has found that the exercise of adjudicative or enforcement jurisdiction under international law over certain events occurring abroad, such as the institution of investigations over the deaths of individuals occurring abroad, may give rise to jurisdiction over *procedural* human rights obligations, such as those arising from the right to life, provided that some 'special features' are present.[219] This brings the notion of human rights jurisdiction closer to the concept of jurisdiction under international law. As the ECtHR has noted recently, this type of jurisdictional link arises especially in instances where the state in question not only has the power to exercise prescriptive or adjudicative powers over events occurring outside of its territory, but also has the obligation to do so under domestic or international law.[220] Likewise, that the event occurred extraterritorially is no obstacle to triggering the obligation to institute the necessary investigative proceedings.[221] This is so to the extent that states may be able to do so through the use of 'international legal assistance and modern technology', for example.[222]

216 Ibid.; see also *Tănase v. Romania*, *supra* note 190, para 136.

217 ECtHR, *McCann and Others v. United Kingdom*, Appl. no. 19009/04, Judgment of 27 September 1995, para 151; *Velasquez Rodriguez v. Honduras*, *supra* note 188, para 167. See also The Netherlands, *Letter of 5 July 2019 (Appendix)*, *supra* note 60, at 4; and Korea, *supra* note 62, at 5.

218 Besson, *supra* note 38, at 5.

219 *Güzelyurtlu and Others*, *supra* note 200, paras 188-190; ECtHR, *Georgia v. Russia (II)*, App. no. 38263/08, Judgement of 21 January 2021, paras 328-332; ECtHR, *Hanan v. Germany*, Appl. no. 4871/16, Judgement of 16 February 2021, paras 132-145.

220 *Georgia v. Russia*, *supra* note 219, para 331; Hanan, *supra* note 219, paras 137-142.

221 Hanan, *supra* note 219, para 145.

222 Ibid.

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 and as widespread as the world's entire population. Thus, it would be unrealistic and unreasonable to expect a state to be in a position to adopt preventive or remedial 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'[223] and constructive knowledge of an immediate and certain risk,[224] 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 the ICT environment. 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.[225] And, as mentioned earlier, when a violation occurs, the have a separate obligation to institute all the necessary proceedings to investigate, punish and redress it.

223 As, for instance, affirmed by the HRC with respect to the right to life. See HRC, *General Comment 36*, *supra* note 42, para. 21; cf. also *Osman v. United Kingdom*, *supra* note 215, paras 115-116.

224 IACtHR, *Sawhoyamaxa Indigenous Community v. Paraguay*, Judgment (Merits, Reparations and Costs), 29 March 2006, para. 155; cf. very similar language in *Tănase v. Romania*, *supra* note 190, para 136.

225 HRC, *General Comment 36*, *supra* note 42, paras 13, 23, 27.

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 the measures required.[226] This is true to the extent that states must prevent objectively foreseeable *threats* to human rights.[227] Thus, a breach of such duty arises from the emergence of a risk of harm, regardless of whether or not it materialises.[228] 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.[229]

226 See, e.g., Ibid., para. 7.

227 Vito Todeschini, 'The Human Rights Committee's General Comment No. 36 and the Right to Life in Armed Conflict', *Opinio Juris*, 21 January 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/.

228 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 42, para. 7; ECtHR, *Keller v. Russia*, Appl. no. 26824/04, Judgment of 17 October 2013, para 82; *Osman v. United Kingdom*, *supra* note 215, 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, paras 13, 14(f), 16). See, generally, Vladislava Stoyanova, 'Fault, Knowledge and Risk Within the Framework of Positive Obligations Under the European Convention on Human Rights', 33 *Leiden Journal of International Law* (2020) 601.

229 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.

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.[230] 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.[231]

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, indiscriminately or disproportionately[232] disable civilian infrastructure and disrupt the provision of services essential to the civilian population. Many states[233] 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.[234] 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.[235] In any event, numerous rules of IHL establish obligations of conduct

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

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

232 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.

233 E.g., United Kingdom (UK) Attorney General's Office, 'Cyber and International Law in the 21st Century', 23 May 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.

234 E.g., *Tallinn Manual 2.0*, *supra* note 6, Rule 82, para 16; *Nuclear Weapons*, *supra* note 25, para 86. See also Helen Durham, 'Cyber operations during armed conflict: 7 essential law and policy questions', *ICRC: Humanitarian Law & Policy*, 26 March 2020, available at https://blogs.icrc.org/law-and-policy/2020/03/26/cyber-armed-conflict-7-law-policy-questions/.

235 See Tilman Rödenhauser, 'Hacking Humanitarians? IHL and the protection of humanitarian organizations against cyber operations', *EJIL:Talk!*, 16 March 2020, at https://www.ejiltalk.org/hacking-humanitarians-ihl-and-the-protection-of-humanitarian-organizations-against-cyber-operations/.

Due diligence in international law and its applicability to ICTs

with which states must comply by exercising due diligence including in their use of ICTs.[236] Some of these require state to prevent violations or harmful activities carried out by third parties, whether states or non-state actors. 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.

i. The general duty to ensure respect for IHL in cyberspace

An obligation containing a standard of due diligence is codified in Article 1 common to the 1949 Geneva Conventions on the protection of victims of war (GCs). It requires states to respect and *ensure respect* for the provisions of the conventions[237] — a provision repeated almost *verbatim* in Article 1(1) of Additional Protocol I (AP).[238] The customary status of this rule was recognized by the ICJ, as well as its application to both international and non-international armed conflict.[239] 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'.[240] According to Rule 144 of the International Committee of the Red Cross (ICRC)'s Customary IHL Study,[241] this obligation requires states not only to refrain from committing or encouraging

236 See Marco Longobardo, 'The Relevance of the Concept of Due Diligence for International Humanitarian Law', 37 *Wisconsin International Law Journal* (2020) 44; 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.

237 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.

238 Article 1(1), AP I.

239 *Nicaragua*, *supra* note 40, para 220; ICRC, *Commentary on the First Geneva Convention* (2016), available at https://ihl-databases.icrc.org/ihl/full/GCi-commentary (hereinafter '2016 Commentary'), Article 1 - Respect for the Convention, at paras 125-126.

240 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.

241 Jean-Marie Henckaerts and Louise 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.

Due diligence in international law and its applicability to ICTs

violations of IHL[242] but also to take positive steps to ensure — even in peacetime[243] — that other entities comply with IHL thereby preventing such violations from occurring.[244]

This obligation also applies in the ICT environment 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,[245] or exerts a reasonable degree of influence, including other states and non-state groups located in different parts of the world.[246] As with other protective obligations, the duty to respect and ensure respect for IHL is triggered and limited by a state's capacity to act.[247] 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.[248]

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, including in their use of ICTs.[249] The duty is triggered not only by a state's knowledge of violations but also by objective foreseeability thereof.[250]

242 ICRC, *2016 Commentary*, *supra* note 239, paras 154 and 158-163.

243 Ibid., paras 127-128 and 185.

244 Ibid., paras 121, 153-154 and 164-173. On this obligation generally, see Knut Dörmann and José 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 236, at 57-60; and Berkes, *supra* note 236, at 442. *Contra*, see Tomasz Zych, 'The Scope of the Obligation to Respect and to Ensure Respect for International Humanitarian Law', 27(2) *Windsor Yearbook of Access to Justice* (2009) 251; and 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. On examples of operational measures, see European Union, 'Updated European Union Guidelines on promoting compliance with international humanitarian law', 2009/C 303/06, 15 December 2009, para. 16.

245 ICRC, *2016 Commentary*, *supra* note 239, para 150.

246 Ibid., paras 150 and 153-154.

247 Ibid., paras 166, 187.

248 Ibid., paras 165-166 and, *mutatis mutandis*, *Bosnian Genocide*, *supra* note 82, para 430. See also Longobardo, *supra* note 236, at 60-62.

249 ICRC, *2016 Commentary*, *supra* note 239, para 187.

250 Ibid., paras 150, 164.

Due diligence in international law and its applicability to ICTs

Nonetheless, although the duty to prevent violations of IHL *arises* from the moment they become known or foreseeable, it appears to be *breached* only if the actual harm materializes, like the Corfu Channel and no-harm principles.[251] 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,[252] demanding its cessation, guarantees of non-repetition or reparations,[253] refraining from recognising the situation as lawful and rendering aid and assistance to the state in breach,[254] as well as taking effective steps to investigate and punish the violations.[255]

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 duties to exercise due diligence in protecting 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.*"[256] 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 the latter often depend on services and resources provided by private entities.[257] The interconnectivity of the Internet and other networks may also mean that cyberattacks directed against military objectives may spill over

251 ICRC, *2016 Commentary*, *supra* note 239, para 166 establishes a parallelism between common Article 1 and Article 1 of the 1948 Genocide Convention. The ICJ in *Bosnian Genocide*, *supra* note 82, 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.

252 ICRC, *2016 Commentary*, *supra* note 239, para 181.

253 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-iraniraq-memoranda.

254 Articles 16 and 40-41, ARSIWA; cf. ICRC, *2016 Commentary*, *supra* note 239, paras 158-163.

255 Koivurova, *supra* note 10, para 32.

256 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.

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

Due diligence in international law and its applicability to ICTs

civilian systems, causing disruption or dysfunctionality.[258]

To obviate such undesirable results, Article 58 AP I requires all 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.[259] The rule has achieved customary status, as recognised by Rules 22-24 of the ICRC's Study on Customary IHL, and is applicable not only in international armed conflict but also, arguably, in non-international ones.[260]

Along with other protective 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'.[261] 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.[262]

258 See Laurent Gisel and Tilman Rodenhäuser, 'Cyber operations and international humanitarian law: five key points', *ICRC: Humanitarian Law & Policy*, 28 November 2019, available at https://blogs.icrc.org/law-and-policy/2019/11/28/cyber-operations-ihl-five-key-points/.

259 Yves Sandoz, Christophe Swinarski and Bruno Zimmermann, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (ICRC, 1987), at 692, para 2239.

260 Henckaerts and Doswald-Beck, *supra* note 241, at 69-70.

261 Cf., e.g., US Department of Defense, 'Law of War Manual', June 2015 (Updated December 2016), at 192, para. 5.2.3.2.

262 Cf. ICRC, *Position Paper*, *supra* note 232, at 6. See also Kubo Mačák, Laurent Gisel and Tilman Rodenhäuser, 'Cyber Attacks against Hospitals and the COVID-19 Pandemic: How Strong are International Law Protections?', *JustSecurity*, 27 March 2020, available at https://www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/.

5. Conclusion: A Patchwork of Existing Duties to Behave Diligently in the ICT Environment

Throughout this chapter, 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.[263] Secondly, and relatedly, those obligations are subject to and limited by a state's capacity to act,[264] giving effect to the idea that states have common but differentiated responsibilities.[265] Thirdly, this flexible obligation of conduct seems to be coupled with an obligation of result[266] to put in place the minimal legislative, judicial and executive infrastructure needed to exercise due diligence.[267] 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.[268] 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

263 *ILA Study*, *supra* note 14, at 5; HRC, *General Comment 36*, *supra* note 42, para. 22.

264 *Alabama*, *supra* note 15, at 129; *ILA Study*, *supra* note 14, at 20, 47; HRC, *General Comment 36*, *supra* note 42, para. 21; *Bosnian Genocide*, *supra* note 82, paras 430-432; *Nicaragua*, *supra* note 40, para 157. See also Koivurova, *supra* note 10, paras 17, 19. On how capacity limits states' ability to prevent and mitigate harmful cyber operations, see OEWG, 'Final Substantive Report', 10 March 2021, UN Doc. A/AC.290/2021/CRP.2 ('OEWG Final Substantive Report'), para 54.

265 Koivurova, *supra* note 10, para 19. On the specific context of ICTs, see OEWG, 'Draft Substantive Report [Zero Draft], A/AC.290/[DATE], 19 January 2021 ('OEWG Zero Draft'), para 86.

266 Pisillo-Mazzeschi, *supra* note 14, at 27.

267 ILC, *Draft Articles on Prevention*, *supra* note 21, at 155-156; Commentary to Article 3, para. 17; Article 5 and Commentary; *ILA Study*, *supra* note 14, at 124; Alabama Claims Commission, 131; Koivurova, *supra* note 10, para 21; Pisillo-Mazzeschi, *supra* note 14, at 26–27; Kolb, *supra* note 36, at 117, 127; Couzigou, 50-51; Okwori, 223.

268 *ILA Study*, *supra* note 14, at 47.

Due diligence in international law and its applicability to ICTs

contrary to the rights of other states, significant transboundary harm, or a violation of more specific international rules, such as IHRL and IHL.

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'.[269] 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'.[270] The International Law Association[271] and some states have also supported this position, particularly in the context of cyberspace.[272] But whether or not this holds true, it should not detract from the fact that a comprehensive legal framework of *binding* obligations to prevent and redress harm already applies in cyberspace, however 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 containing a standard of due diligence belonging to specialised 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.

269 Emphasis added. *Pulp Mills*, *supra* note 14, para 101. See also *ILA Study*, *supra* note 14, at 6; Koivurova, *supra* note 10, para 41; Couzigou, *supra* note 96, at 39; Olivia Hankinson, 'Due Diligence and the Gray Zones of International Cyberspace Laws', *MJIL Online*, 2018, available at http://www.mjilonline.org/due-diligence-and-the-gray-zones-of-international-cyberspace-laws/.

270 *Trail Smelter*, *supra* note 22, at 1963 and 1965.

271 *ILA Study*, *supra* note 14, at 6.

272 See, e.g., France, *Response to the OEWG pre-draft report*, *supra* note 55, at 3; Korea, *supra* note 62, at 2, 5; 'International law and cyberspace: Finland's national positions', 15 October 2020, available at https://um.fi/documents/35732/0/Cyber+and+international+law%3B+Finland%27s+views.pdf/41404cbb-d300-a3b9-92e4-a7d675d5d585?t=1602758856859, at 4.

Due diligence in international law and its applicability to ICTs

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, 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. However, 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. This is because 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.

Cyber due diligence in practice

1. Introduction: Mapping out Diligent State Behaviour in the ICT Environment

In this chapter, we turn to the application of the 'patchwork of cyber due diligence obligations' in practice. As argued in Chapter 1, we believe that applying rules of general international law to ICTs can be more realistically framed as a process of *interpretation*, as opposed to the identification of new, technology-specific customary rules. Interpretation is an inherent part of legal reasoning, which is set in motion not only when abstract legal concepts are assessed but also when these are applied to facts of life – old and new. Thus, in Chapter 4, we laid out the existing rules of international which we believe apply to ICTs *by default*, given their general scope of application. Yet to ensure that this reading of the patchwork of due diligence duties is consistent with states' current behaviour and attitudes in their use of ICTs, we have also looked at a geographically representative sample of behaviour and position statements adopted by states across the globe.

Those materials, which we conveniently call 'subsequent behaviour and attitudes' constitute an important tool for the interpretation of evolving customary and treaty rules. In the same vein, by matching our 'deductive' findings with current state practice and expressions of *opinio juris*, we also confirm them by induction. Specifically, we have looked at different measures adopted by a number of states at the domestic and international levels which can be said to amount to diligent behaviour in the ICT environment. We started with an in-depth analysis of measures taken by a representative sample of states selected on the basis of their legal traditions, geographical representation, cyber influence and capabilities, as well as the availability of relevant data. These are: Japan, China, Singapore, Russia, the United Kingdom, Germany, France, the United States, Canada, Brazil, Argentina, South Africa, Iran and Australia.[1] We looked at domestic laws, regulations, policy and strategic documents, country-wide initiatives, implementation practices,

1 We would like to acknowledge that the United Nations Institute for Disarmament Research (UNIDIR) Cyber Policy Portal (available at https://unidir.org/cpp/en/) was instrumental to our survey.

Cyber due diligence in practice

bilateral and multilateral treaties, and official statements before international fora which constitute examples of diligent behaviour as well as states' attitudes towards these measures. Subsequently, we carried out less-comprehensive surveys of the same or similar materials with respect to other states which have so far expressed their views on cyber due diligence.

On the basis of this data, which we describe below, we have found that an overwhelming number of states have implemented measures of diligent behaviour in cyberspace, more often than not with the understanding that they must do so under international law, though without pinpointing the exact source of their obligation. Ostensibly, when states have put forward their own understanding of due diligence in their use of ICTs, they have not always been consistent in identifying its exact legal basis and content under international law. For instance, states such as the Netherlands,[2] Finland,[3] France[4] and Czech Republic[5] seem to have conflated the requirements of the Corfu Channel and no-harm principles into a single cyber due diligence rule, following the approach of the Tallinn Manuals.[6] Nevertheless, taken as a whole, there is no question that both the diligent practice and the agreement that this practice is required by binding international law, can be observed among a significant number of states. This should put to rest any doubts about the existence and applicability of protective duties containing a standard of due diligence to ICTs.

2 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', 5 July 2019, available at https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace ('Netherlands Letter').

3 'International law and cyberspace – Finland's national positions', 15 October 2020, available at https://um.fi/documents/35732/0/Cyber+and+international+law%3B+Finland%27s+views.pdf/41404cbb-d300-a3b9-92e4-a7d675d5d585?t=1602758856859 ('Finland's Position'), at 4.

4 'France's response to the pre-draft report from the OEWG Chair', April 2020, available at https://www.un.org/disarmament/open-ended-working-group/ (France's response), at 3.

5 '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', 11 March 2020, available at https://front.un-arm.org/wp-content/uploads/2020/04/czech-republic-oewg-pre-draft-suggestions.pdf ('Comments by the Czech Republic'), at 3.

6 Michael Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013), at 26, Rule 5; Michael Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), at 30, Rule 6.

In the remainder of this chapter, we provide detailed guidance on the implementation of those obligations. Such guidance was drawn from our survey of diligent state behaviour around the world. It consists of a rich 'roadmap' of measures at the disposal of states in ensuring compliance with different protective duties in their use of ICTs. Indeed, to ensure that states do comply with their patchwork of cyber due diligence obligations, it is not enough to demonstrate the existence of these rules and flesh out their content and elements *in the abstract*, as we have done in previous chapters. Clearer guidance ought to be provided as to how states should interpret, apply and implement due diligence duties in the ICT environment.

Having said that, the conclusions we draw on particular cyber due diligence measures remain *guidelines* rather than binding international law requirements. As with any due diligence obligation, general or specific, states enjoy a wide margin of discretion in discharging their preventive or remedial duties in respect of ICTs.[7] And their responsibility for breaches of those obligations must be assessed on a case-by-case basis, by considering, *inter alia*, their knowledge of the harm or risk in question and the measures which they were reasonably capable of adopting in the circumstances.

2. A Roadmap to Compliance: Key Cyber Due Diligence Measures

States enjoy a wide margin of discretion when discharging their due diligence duties in cyberspace. This is so to the extent that such obligations are limited by the duty-bearer's capacity to act. Correspondingly, a large spectrum of cyber due diligence measures of various types, costs and aims is available to states. The more feasible a measure is, the higher the expectation on a state to adopt it. Thus, basic measures which are inherent to statehood and thus available to each and every state, such as legislation, investigation and prosecution of crimes committed through ICTs (i.e., 'cybercrime'), might be

7 See Schmitt, Tallinn Manual 2.0, supra note 6, at 44, Commentary to Rule 7, para 6.

Cyber due diligence in practice

necessary to fulfil a state's minimum capacity-building obligations under international law.[8] By contrast, more costly and sophisticated measures may not be feasible for many states, especially less developed countries. Despite their differences, these measures have in common the ability to prevent, stop and/or redress the effects of harmful cyber activity, with varying levels of effectiveness. For the sake of consistency and simplicity, we have arranged those measures largely in accordance with the classification devised by the ITU's Global Cybersecurity Agenda. These are: a) legal measures; b) technical and procedural measures; c) organisational or institutional structures; d) capacity-building; e) international cooperation;[9] with the additional category of f) financial measures.

Naturally, these categories overlap as certain measures either have a dual nature or are interdependent. For instance, legal measures such as legislation, investigation and prosecution ground, enforce and adjudicate technical measures (such as ICT standards and monitoring), organisational structures (such as public-private partnerships), capacity-building (such as training and public awareness campaigns), and international cooperation between states. In the same vein, the implementation of legal, technical, capacity-building and cooperative measures depends on joint efforts and institutional arrangements between governmental bodies operating at different domestic levels, state diplomats, the industry, academia and civil society.[10] And these multi-stakeholder efforts can only work if experts in different fields, such as law, policy, politics and computer science work together in a collaborative way. After all, even if only states have binding due diligence obligations *under international law*, the vast majority of ICTs,

8 On how this bare minimum or baseline obligation applies in cyberspace, see Russel Buchan, Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm', 21 *Journal of Conflict & Security Law* (2016) 429, at 436-437; Robert Kolb, Reflections on Due Diligence Duties and Cyberspace', 58 *German Yearbook of International Law* (2015) 113, at 127. See Riccardo Pisillo-Mazzeschi, 'The Due Diligence Rule and the Nature of the International Responsibility of States', 35 *German Yearbook of International Law* (1992) 9, at 26-27; 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 155, Commentary to Article 3, paras 15-17.

9 ITU Global Cybersecurity Agenda (GCA), High-Level Experts Group (HLEG), Report of the Chairman of the HLEG (2008), available at https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx ('ITU GCA Report'), at 2-3.

10 See UK Multi-stakeholder Advisory Group on Cyber issues, 'Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015', available at https://www.un.org/disarmament/wp-content/uploads/2019/12/efforts-implement-norms-uk-stakeholders-12419.pdf, 4 December 2009, at 5.

Cyber due diligence in practice

including the Internet and its public core (i.e. the Internet Protocol Addresses, the Domain Name System, fibre optic or copper cables spread across national borders, routers and their routing protocols, Internet Exchange Points),[11] are owned or controlled by private tech companies and used by individuals in civil society.[12]

Measures can address domestic or external threats and be of a proactive or defensive nature. For instance, to prevent their territory from being used by malicious actors to harm other states or their populations, states may adopt a number of legal, technical, organisational, capacity-building and cooperative measures, in line with the Corfu Channel and no-harm principles, as well as human rights obligations within their jurisdiction.[13] In the same vein, to protect their own territory and population from external cyber threats and thereby fulfil their duties to protect human rights and protect civilians during armed conflict, states may adopt a range of legal, technical, organisational, capacity-building, cooperative and financial measures. Not surprisingly, these various measures reflect, to a large extent, those which states would be expected to adopt to implement the various norms of responsible state behaviour in cyberspace, listed in para 13 of the 2015 GGE Report.[14]

a. Legal Measures

Legal measures form the bedrock of cyber due diligence, both as a matter of law and policy. An appropriate legal and regulatory framework appears as an indispensable step for the effective

11 Global Commission on the Stability of Cyberspace, 'Definition of the Public Core, to which the Norm Applies', May 2018, available at https://cyberstability.org/wp-content/uploads/2018/07/Definition-of-the-Public-Core-of-the-Internet.pdf.

12 See ITU GCA Report, *supra* note 9, at 8, para 1.12. On the role of private companies in tackling malicious cyber operations, see, e.g., Tom Burt, 'Cyberattacks targeting health care must stop', *Microsoft On the Issues*, 13 November 2020, available at https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/.

13 On extraterritorial human rights jurisdiction over activities of third parties located in a state's territory with effects abroad, see, e.g., 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 22; 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.

14 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.

Cyber due diligence in practice

prevention, response to and mitigation of online threats and harms. On the one hand, several preventive and remedial measures of a legal, judicial or executive nature carry with them limitations on the rights of individuals and private entities, which require prior notice under international or domestic law.[15] In particular, the criminalisation of malicious cyber activity, such as ransomware, spyware, phishing or cyber terrorism requires prior criminal law, in accordance with the principle of legality, enshrined in virtually all human rights treaties and legal systems across the world.[16] Likewise, the imposition of obligations or liability on companies to remedy any harm resulting from their activities in cyberspace must be done by law.[17] On the other hand, from a policy perspective, it is hard to implement measures of cyber due diligence without a constant, guiding legal framework. In this sense, law serves to provide direction and structure to other measures. In the same vein, a clear legal framework laying out the rights and responsibilities of states and private entities in the cyber domain, along with sanctions and remedies in case of non-compliance, is a powerful means to induce compliance, by educating the public, deterring malicious activity and punishing those responsible.[18] According to the experts who contributed to the ITU's Global Cybersecurity Agenda, effective legal instruments are essential to build confidence and security in the use of ICTs.[19] Such legal measures include not only legislation and statutes, but legal principles, customary rules, regulation, adjudication — whether through judicial, arbitral

15 Antonio Coco and Talita de Souza Dias, 'Cyber Due Diligence in Public Health Crises', in Carla Ferstman and Andrew Fagan, *Covid-19, Law and Human Rights: Essex Dialogues, A Project of the School of Law and Human Rights Centre* (Creative Commons, 1 July 2020), available at http://repository.essex.ac.uk/28002/, at 304. See also, in the context of international human rights law, ECtHR, *Bărbulescu v. Romania*, Appl. no. 61496/08, Judgment of 12 January 2016, paras 115-116; 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 ('General Comment 31'), paras 7, 13; General Comment 36, *supra* note 13, paras 4, 13, 22.

16 See, e.g., Art. 15, International Covenant on Civil and Political Rights 1966, 999 UNTS 171; Art 7, European Convention for the Protection of Human Rights and Fundamental Freedoms1953, ETS 5; Art 9, American Convention on Human Rights 1978, OAS Treaty Series No 36, 1144 UNTS 123. See generally Kenneth S Gallant, *The Principle of Legality in International and Comparative Criminal Law* (Cambridge University Press, 2010).

17 See UN General Assembly, 'Declaration of the High-level Meeting of the General Assembly on the Rule of Law at the National and International Levels', A/RES/67/1, 30 November 2012, para 2.

18 Tech Accord in Australia's Department of Foreign Affairs and Trade, 'Public Consultation: responsible state behaviour in cyberspace in the context of international security: Summary of public submissions on developing best practice guidance on implementation of the 11 norms of responsible state behaviour in cyberspace […]', 4 November 2019, available at https://www.dfat.gov.au/sites/default/files/compilation-norm-implementation-guidance.pdf ('Australia's Public Consultation'), at 9.

19 ITU GCA Report, *supra* note 9, at 6.

Cyber due diligence in practice

or alternative means of dispute resolution — and law enforcement. And these can be enacted, developed or instituted at the domestic or international level.

Given the transboundary nature of cyberspace, a comprehensive international legal framework is instrumental to constrain and redress malicious cyber operations. Similarly, while harmonised domestic legal frameworks criminalising or outlawing such operations would be ideal,[20] extradition, law enforcement and judicial cooperation agreements can help secure legal compliance across national borders.[21] International and domestic legal frameworks may well be technology-specific, but existing legal provisions of a general scope covering a spectrum of technologies may well be effective.[22] To be sure, not all malicious cyber operations do or should constitute cybercrimes, but only the most serious ones, with tort, contract and administrative law covering less harmful activity.[23] For ITU experts, legislative, judicial and law enforcement efforts should focus on spam, identity theft, massive and coordinated cyberattacks against critical information infrastructure, as well as their preparatory acts.[24] Other experts have warned about the need to adopt legal measures to address cyberattacks against digital supply chains,[25] unlawful surveillance, including through spyware software,[26] electoral

20 Ibid, at 6-7, paras 1.1-1.5.

21 Ibid, at 8, paras 1.13 and Tech Accord, at 5.

22 ITU GCA Report, *supra* note 9, at 7, para 1.6.

23 See generally, Lawrence Lessig, 'The Law of the Horse: What Cyberlaw Might Teach', 113 (1999) *Harvard Law Review* 501, at 502.

24 ITU GCA Report, *supra* note 9, at 7, 1.7.

25 See Brad Smith, 'A moment of reckoning: the need for a strong and global cybersecurity response', *Microsoft On the Issues*, 17 December 2020, available at https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/ (arguing that recent IT supply chain attack against SolarWinds software did not just constitute "espionage as usual" but 'a serious technological vulnerability for the United States and the world', affecting the 'trust and reliability of the world's critical infrastructure').

26 See UN Office of the High Commissioner for Human Rights, 'UN experts call for investigation into allegations that Saudi Crown Prince involved in hacking of Jeff Bezos' phone', 22 January 2020, available at https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25488; CitizenLab, 'NSO Group / Q Cyber Technologies: Over One Hundred New Abuse Cases', 29 October 2019, available at https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/.

Cyber due diligence in practice

interference[27] and online disinformation campaigns.[28]

Thus, in a somewhat circular way, compliance with due diligence obligations under international law necessitates, at the very least, more clarity as to the extent to which existing international law applies in cyberspace, particularly overarching rules and principles such as sovereignty and non-intervention.[29] In this regard, several scholars,[30] international organisations,[31] NGOs and industry representatives,[32] have called upon states to express their views as to how international law applies in cyberspace. All the states we have surveyed have been quite vocal in this respect. In particular, France[33] and Australia[34] have not only made detailed submissions before international fora, such as the GGE and Open-Ended Working Group (OEWG) on ICTs but have also published comprehensive documents laying out their positions on the applicability, scope and interpretation of core international legal

27 See 'The Oxford Statement on International Law Protections Against Foreign Electoral Interference Through Digital Means', 27 October 2020, available at https://www.elac.ox.ac.uk/the-oxford-statement-on-international-law-protections-against-foreign-electoral-interference-through.

28 See, e.g., EU Code of Practice on Disinformation, September 2018, available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454; EU, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Tackling online disinformation: a European Approach', 26 April 2018, available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0236&from=EN.

29 Australia's Public Consultation, *supra* note 18, at 2-3, 5, 8-9, 12, 17 (comments by Institute for International Cyber Stability, Tech Accord, Australian Strategic Policy Institute, International Cyber Policy Centre and Microsoft).

30 Przemysław Roguski, 'Application of International Law to Cyber Operations: A Comparative Analysis of States' Views', Policy brief: The Hague Program for Cyber Norms, March 2020, at 1; Michael Schmitt, 'Grey Zones in the International Law of Cyberspace', (2017) 42 *Yale Journal of International Law Online* 1, at 20-21.

31 EU Statement – United Nations 1st Committee: Thematic Discussion on Other Disarmament Measures and International Security, 26 October 2018, available at https://eeas.europa.eu/delegations/un-new-york/52894/eu-statement-%E2%80%93-united-nations-1st-committee; Organization of American States (OAS), Improving Transparency — International Law and State Cyber Operations: Fourth Report (Presented by Prof. Duncan B. Hollis), OEA/Ser.QCJI/doc. 615/20 rev.1 7 August 2020 ('Improving Transparency'), para 10.

32 See *supra* note 29.

33 France's response, *supra* note 4; France, Ministry of Defence, 'Droit International Appliqué Aux Opérations Dans Le Cyberespace', 9 September 2019, available at https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqu%C3%A9+aux+op%C3%A9rations+Cyberespace.pdf; Statement by France's Deputy Permanent Representative at the UN at the UNSC Arria-Formula Meeting on Cybersecurity, Ms. Anne Gueguen, 22 May 2020, available at https://youtu.be/K704P5D1n3E, timestamp 25:00; 'France, 'Stratégie internationale de la France pour le numérique', 2 April 2020, available at https://www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf.

34 Australian Department of Foreign Affairs and Trade (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; 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.

Cyber due diligence in practice

rules and principles in cyberspace. Similarly, the UK has issued several statements and submissions conveying its position on questions of general international law, such as sovereignty, non-intervention, the use of force and IHL in cyberspace.[35]

And all other sampled states have at the very least publicly articulated their views on discrete issues regarding the applicability and/or interpretation of international law to ICTs, including, in particular, with respect to cyberattacks against the healthcare sector.[36]

At the interface between international and domestic law are certain international treaties requiring states to criminalise, investigate and prosecute malicious cyber conduct domestically, as well as to cooperate for this purpose. A prime example of this sort is the Council of Europe's Budapest Convention on Cybercrime,[37] which,

35 E.g., 'Cyber and International Law in the 21st Century, Speech by United Kingdom Attorney General Jeremy Wright QC *MP*', 23 May 2018, available at https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century ('UK 2018 Speech'); Non-Paper on Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015, 1 September 2019, available at https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/uk-un-norms-non-paper-oewg-submission-final.pdf ('UK Non-Paper'); 'UK response to Chair's initial 'Pre-draft' of the report of the OEWG on developments in the field of information and telecommunications in the context of international security', April 2020, available at https://front.un-arm.org/wp-content/uploads/2020/04/20200415-oewg-predraft-uk.pdf.

36 See, e.g., 'Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security - Comments by ARGENTINA, 1 April 2020', available at https://front.un-arm.org/wp-content/uploads/2020/04/oewg-ict-comments-argentina-3.pdf; 'Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, Second Substantive Session - New York, 11 February 2020, Statement by the Delegation of Brazil, INTERNATIONAL LAW', 11 February 2020, available at http://webtv.un.org/search/4th-meeting-open-ended-working-group-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-second-substantive-session-10%E2%80%9314-february-2020/6131734500001/?term=%22Open%20Ended%20Working%20Group%22&lan=English&cat=Meetings%2FEvents&sort=date, timestamp 0:15:45 ('Brazil's OEWG Statement'); 'New Canadian text proposals (to the OEWG's initial pre-draft)', 6 April 2020, available at https://front.un-arm.org/wp-content/uploads/2020/04/new-canadian-text-proposals-april-6-final.pdf ('Canada's Proposals on OEWG pre-draft'); 'China's Contribution to the Initial Pre-Draft of OEWG Report', March 2020, available at https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf; Germany, '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', 6 April 2020, available at https://front.un-arm.org/wp-content/uploads/2020/04/20200401-oewg-german-written-contribution-to-pre-draft-report-1.pdf ('Germany's Comments on OEWG pre-draft'); 'Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace', 1 July 2020, available at https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat; '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"', April 2020, available https://front.un-arm.org/wp-content/uploads/2020/04/japan-comments-on-oewg-pre-draft.pdf; 'COMMENTARY OF THE RUSSIAN FEDERATION ON THE INITIAL "PRE-DRAFT" OF THE FINAL REPORT OF THE UNITED NATIONS OPEN-ENDED WORKING GROUP ON DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY', April 2020, available at https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf; 'Statement by the South African Representative at the UNSC Arria Formula Meeting on Cyber Attacks against Critical Infrastructure', 26 August 2020, available at https://www.youtube.com/watch?v=CbBchZEG5D8, timestamp 1:28:00.

37 See also Australia's Public Consultation, *supra* note 18, at 2, 4-7 (submissions by Tech Accord, Microsoft, Australian Strategic Policy Institute, International Cyber Policy Centre).

Cyber due diligence in practice

among our surveyed states, has been ratified by France, Germany, the UK, the US, Japan and Argentina.[38] Several legal experts involved in the ITU's Global Cybersecurity Agenda have cited it as a model for states in the adoption of domestic rules and principles for the prevention and punishment of cybercrime.[39] The Budapest Convention has also been supplemented by an Additional Protocol Concerning the Criminalisation of Acts of a or Xenophobic Nature Committed Through Computer Systems.[40] Other examples include: the Commonwealth of Independent States' 2001 Agreement on Cooperation in Combating Offences related to Computer Information;[41] the Shanghai Cooperation Organization's 2009 Agreement on Cooperation in the Field of International Information Security;[42] the 2010 Arab Convention on Combating Information Technology Offences;[43] and the African Union Convention on Cyber Security and Personal Data Protection, which was adopted in 2014 and has not yet entered into force.[44] Although other multilateral treaties on cybercrime are yet to be concluded, several states have concluded bilateral agreements or memoranda of understanding stressing their commitment or intention to criminalise, prosecute and punish malicious cyber activity, including the states we have surveyed.[45]

38 Council of Europe, 'Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY', available at https://www.coe.int/en/web/cybercrime/parties-observers.

39 ITU GCA Report, *supra* note supra note 9, at 6-8.

40 ETS 189.

41 Available in English at https://dig.watch/instruments/agreement-cooperation-combating-offences-related-computer-information-commonwealth-independent.

42 Concluded on 16 June 2009, available at http://eng.sectsco.org/documents, download at http://eng.sectsco.org/load/207508/.

43 Available in Arabic at http://www.lasportal.org/ar/legalnetwork/Pages/typicalarablaws.aspx. English text available at https://dig.watch/instruments/arab-convention-combating-technology-offences. It appears that the Convention entered into force in 2014. See https://www.unescwa.org/sites/www.unescwa.org/files/uploads/policy-recommendations-cybersafety-arab-region-summary-english.pdf, at 3. The similarity between the Arab Convention and the Budapest Convention has been noted in Hakmeh, 'Cybercrime and the Digital Economy in the GCC Countries', *Chatham House Research Paper*, 2017, available at https://www.chathamhouse.org/sites/default/files/publications/research/2017-06-30-cybercrime-digital-economy-gcc-hakmeh.pdf, at 11 and Annex 1.

44 See https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection. Provisions related to adequate cybercrime legislation most notably include Arts 25 and 29-31. When in force, the Convention will oblige Parties also — *inter alia* — to ensure the safety of electronic transactions (Arts 2-7) and the protection of personal data (Arts 8-23). Other notable obligations include: the adoption of a national cybersecurity framework (Art. 24); the establishment of adequate institutional mechanisms in charge of national cybersecurity governance (Art. 27); and international cooperation (Art. 28).

45 E.g., 'Argentina, Brazil agree on cyber-defense alliance against US espionage', 15 September 2013, available at https://www.rt.com/news/brazil-argentina-cyber-defense-879/; 'Agreement on Strategic Cooperation between the Federative Republic of Brazil and the European Police Office',

Cyber due diligence in practice

When it comes to domestic law, all sampled states have put in place a legal framework laying out measures to prevent, stop and respond to cyber harms, although these vary in scope and detail.[46] They have

11 April 2017, available at https://www.europol.europa.eu/agreements/brazil-0; 'Cybersecurity Action Plan Between Public Safety Canada and the [US] Department of Homeland Security', October 2012, available at https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cybrscrt-ctn-plan/index-en.aspx; 'Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on cooperation in ensuring international information security', 30 April 2015, available at https://cyber-peace.org/wp-content/uploads/2013/05/RUS-CHN_CyberSecurityAgreement201504_InofficialTranslation.pdf; 'Vision commune du président de la République française, Emmanuel Macron et du premier ministre d'Australie, Malcolm Turnbull sur la relation franco-australienne', 2 May 2018, available at https://www.diplomatie.gouv.fr/fr/dossiers-pays/australie/evenements/article/vision-commune-du-president-de-la-republique-francaise-emmanuel-macron-et-du; 'First U.S.-China Law Enforcement and Cybersecurity Dialogue', 6 October 2017, available at https://www.dhs.gov/news/2017/10/06/first-us-china-law-enforcement-and-cybersecurity-dialogue; 'Singapore Signs Memorandum of Cooperation on Cybersecurity Capacity Building with the United Kingdom', 17 April 2018, available at https://www.csa.gov.sg/news/press-releases/singapore-signs-memorandum-of-cooperation-on-cybersecurity-capacity-building-with-the-united-kingdom#sthash.4FVrxTRY.dpuf; 'UN – Fight against terrorism/cyber security/digital technology/high-level meeting on preventing terrorist use of the Internet – Joint statement by the United Kingdom, France and Italy', 20 September 2017, available at https://uk.ambafrance.org/France-UK-and-Italy-cooperate-to-fight-terrorism-online; 'Joint UK-Australia Statement on Cyber Co-operation', 11 July 2017, available at https://www.gov.uk/government/news/joint-uk-australia-statement-on-cyber-co-operation; 'Press release on signing a cooperation agreement between the Government of the Russian Federation and the Government of the Republic of South Africa on maintaining international information security', 4 September 2017, available at https://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2854430; 'Joint Communiqué of the 13th Joint Commission between the Republic of South Africa and the Islamic Republic of Iran held in Pretoria on 23 October 2017 (corresponding to 1 Aban 1396)', available at http://www.dirco.gov.za/docs/2017/iran1023.htm. More bilateral agreements are surveyed at Theresa Hitchens and Nilsu Goren, 'International Cybersecurity Information Sharing Agreements', Center for International and Security Studies at Maryland, Phase I Study Report, October 2017, available at https://cissm.umd.edu/sites/default/files/2019-07/Cyber information sharing agreement report - 102017 - FINAL.pdf.

46 Decreto 577/2017 (Argentina), available at http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/277518/norma.htm; Law No. 12.965 ('Marco Civil da Internet'), 23 April 2014 (Brazil), available at https://www.publicknowledge.org/documents/marco-civil-english-version; Telecommunications and Other Legislation Amendment Act of 2017 (Australia), available at https://www.legislation.gov.au/Details/C2017A00111; Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5) (Canada), available at https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html; Cybersecurity Law (China), 1 June 2017, available at https://www.chinalawtranslate.com/bilingual-2016-cybersecurity-law/?lang=en; National Security Law (China), 1 July 2015, available at https://www.chinalawtranslate.com/2015nsl/?lang=en; LOI n° 2018-133 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité (France), 26 February 2018, available at https://www.legifrance.gouv.fr/loda/id/JORFTEXT000036644772; LOI n° 2016-1321 pour une République numérique (France), 7 October 2016, available at https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033202746/; Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung), 21 June 2017 (Germany), available at https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s1903.pdf; Telecommunications Act (Telekommunikationsgesetz, TKG), 27 June 2017 (Germany), available at https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s1963.pdf; Computer Crimes Act (Law No. 71063), 26 May 2009 (Iran), available at https://internetlegislationatlas.org/#/countries/Iran/frameworks/internet-regulation (but freedom of expression concerns have been voiced against this law; see, e.g., ARTICLE 19, 'Islamic Republic of Iran: Computer Crimes Law', 2012), available at https://www.article19.org/data/files/medialibrary/2921/12-01-30-FINAL-iran-WEB%5B4%5D.pdf; General Framework for Secure IoT Systems, 26 August 2016 (Japan), available at https://www.nisc.go.jp/eng/pdf/iot_framework2016_eng.pdf; Basic Act on Cybersecurity, 12 November 2014 (Japan), available at http://www.japaneselawtranslation.go.jp/law/detail/?printID=&re=02&vm=02&id=2760&lvm=01; Federal Law N. 276-FZ on Amendments to the Federal Law on Information, Information Technologies and Information Protection, 29 July 2017 (Russia), available at http://www.consultant.ru/document/cons_doc_LAW_220885/; Federal Law N. 187-FZ on the Security of Critical Information Infrastructure, 26 July 2017 (Russia), available at http://www.consultant.ru/document/cons_doc_LAW_220885/; Federal Law N. 149-FZ on Information, Information Technologies and Information Protection, 27 July 2006 (Russia), available at http://www.consultant.ru/document/cons_doc_LAW_220885/; Cybersecurity Act, 2 March 2018 (Singapore), available at https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312; Electronic Communications and Transactions Act No. 25, 2 August 2002 (South Africa), available at https://www.gov.za/documents/electronic-communications-and-transactions-act; The Network and Information Systems Regulations 2018, 10 May 2018 (UK), available at https://www.legislation.gov.uk/uksi/2018/506/made; Electronic Communications Act 2000, 25 May 2000 (UK), available at https://www.legislation.gov.uk/ukpga/2000/7/pdfs/ukpga_20000007_en.pdf; Cybersecurity Act of 2015 (also known as Cybersecurity Information Sharing Act), 18 December 2015 (US), available at https://epic.org/privacy/cybersecurity/Cybersecruity-Act-of-2015.pdf; Cybersecurity Enhancement Act of 2014, 18 December 2014 (US), available at https://www.congress.gov/113/plaws/publ274/PLAW-113publ274.pdf. At the European Union level, it was also felt that a common legal framework on cybersecurity was needed. For such reason, in 2016, the EU adopted the so-called NIS Directive (Directive on security of network and information systems), which member States had to transpose into national legislation within about 2 years. Among other things, the NIS Directive aimed at ensuring members' preparedness to respond to cybersecurity incidents, for instance by establishing competent national authorities and Computer Security Incident Response Teams (CSIRTs). See Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG.

Cyber due diligence in practice

all adopted specific criminal provisions on cybercrime, including, in particular, offences affecting the availability, confidentiality and integrity of computer systems and/or data, as well as the dissemination of harmful content, such as child pornography, terrorism, advocacy for hatred, or malicious software.[47] Some have adopted legislation allowing the imposition of targeted sanctions — in the form of asset freezes and travel bans against individuals and entities involved in harmful cyber operations, in order to deter and counter them.[48] A large majority of states have issued national cyber security strategies, outlining key aims and measures to promote a safe online environment. Notable among these are the protection or defence of public and private systems,[49] particularly critical infrastructure;[50] detection, prevention and response to, and recovery from cyber incidents,[51] attacks,[52] threats,[53] or acts

47 Law no 26.388, 28 July 2017 (Argentina), available at http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm; Cybercrime Legislation Amendment Act 2012, No. 120, Schedule 3 (Computer offences amendments), 12 September 2012 (Australia), available at https://www.legislation.gov.au/Details/C2012A00120; Law no 12.737 of 2012 (adds Art. 154-A to the 1940 Criminal Code) (Brazil), available at http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm#art2; Criminal Code of 1985 (Canada), ss. 487.0194, 342.1, 342.2, 430 (1.1), available at https://laws-lois.justice.gc.ca/Search/Search.aspx?txtS3archA11=computer&txtT1tl3=%22Criminal+Code%22&h1ts0n1y=0&ddC0nt3ntTyp3=Acts; Criminal Law of the People's Republic of China, 14 March 1997, Arts 285-287, available at https://www.fmprc.gov.cn/ce/cgvienna/eng/dbtyw/jdwt/crimelaw/t209043.htm; Code Pénal (France), Arts 222-16, 226-15-226-24, 322-6-1, 432-9, available at https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/2020-11-16/; Unauthorized Computer Access Law, Law n° 128 of 1999 (Japan), available at https://www.cybercrimelaw.net/Japan.html; Computer Misuse and Cybercrime Act 2003 (Act No. 22 of 2003), 30 July 2003 (Iran), available at http://cyber.police.ir/uploads/cyber.pdf; Computer Crimes Act (Law No. 71063) (n 46) (Iran), available at https://internetlegislationatlas.org/#/countries/Iran/frameworks/internet-regulation; Criminal Code, 13 June 1996 (Russia), Arts 271-274, available at http://visalink-russia.com/criminal-code-russian-federation.html; Computer Misuse Act, revised on 31 July 2007 (Singapore), Part II, available at https://sso.agc.gov.sg/Act/CMA1993; Electronic Communications and Transactions Act No. 25, 2 August 2002 (South Africa), Chapter XIII, available at https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf; Computer Misuse Act 1990 (UK), ss. 1-3A, available at https://www.legislation.gov.uk/ukpga/1990/18/contents; Computer Fraud and Abuse Act (18 USC 1030), 1986 (US), available at https://www.energy.gov/sites/prod/files/cioprod/documents/ComputerFraud-AbuseAct.pdf.

48 https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/# (European Union); https://home.treasury.gov/system/files/126/cyber2_eo.pdf; https://home.treasury.gov/system/files/126/cyber_eo.pdf; more at https://www.state.gov/cyber-sanctions/ (US); https://www.gov.uk/government/collections/uk-cyber-sanctions (UK).

49 National Cyber Security Strategy, 2018 (Canada), available at https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx.

50 National Cyberspace Security Strategy, 1 December 2016 (China), available at https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/; National Digital Security Strategy, 16 October 2015 (France), available at https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf; New Strategy for Development of Information Society, 2017 (Russia), available at https://jamestown.org/program/russia-adopts-new-strategy-development-information-society/; Cybersecurity Strategy 2018 (Japan), at 24, available at https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf.

51 National Cybersecurity Strategy (E-Ciber), 5 February 2020 (Brazil), available at http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Decreto/D10222.htm.

52 National Cybersecurity Policy Framework, 4 December 2015 (South Africa), available at https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf; National Cyber Security Strategy, 2018 (Canada), available at https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx.

53 National Cybersecurity Strategy, National Cybersecurity Committee (Comité de Ciberseguridad), 28 May 2019 (Argentina), available at https://www.boletinoficial.gob.ar/detalleAviso/primera/208317/20190528; Cybersecurity Strategy 2018 (Japan), *supra* note 50, at 22-23.

Cyber due diligence in practice

contrary to the maintenance of international security and stability;[54] preparedness, response and recovery.[55] Some states have also adopted a national cyber defence strategy, either as a separate document,[56] or as part of a general military instrument,[57] which recognises the use of ICTs for military purposes, offensive and/or defensive.

Among these, the US, the UK and Japan have published elaborate cyber defence strategies grounded in the idea that it is essential to proactively defend their national ICT systems and infrastructure against malicious cyber operations. Rather than waiting and reacting to cyber attacks, these states have granted national cybersecurity bodies and certain private entities the power to pre-empt cyber threats by actively disrupting and disabling, including by automated means, malware and their infrastructure at the source, before they can be deployed for malicious purposes.[58]

54 National Cyberspace Security Strategy (China), *supra* note 50.

55 The Network and Information Systems Regulations 2018 (UK), *supra* note 46, at Part 2: The National Framework.

56 Defense and National Security Strategic Review 2017 (France), 15 October 2017, available at https://espas.secure.europarl.europa.eu/orbis/document/defence-and-national-security-strategic-review-2017; National Cyber Security Strategy 2016-2021(UK), available at https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 ('UK National Cyber Security Strategy'); Department of Defense Cyber Strategy, 2018 (US), available at https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF ('2018 DoD Cyber Strategy').

57 Libro Blanco de la Defensa, 2015 (Argentina), Chapters I and V, available at https://info.undp.org/docs/pdc/Documents/ARG/libro_blanco_2015.pdf; Defence White Paper 2016 (Australia), Chapters Two and Four, available at https://www.defence.gov.au/WhitePaper/Docs/2016-Defence-White-Paper.pdf; Livro Branco de Defesa National, 2020 (Brazil), at 23 and 46, available at https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/livro_branco_congresso_nacional.pdf; China's Military Strategy, May 2015, available at http://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm; Defense of Japan Pamphlet (Annual White Paper), 2019, at 11, available at https://www.mod.go.jp/en/publ/w_paper/wp_2019.html; National Security Concept of the Russian Federation, December 2015, available at http://www.scrf.gov.ru/security/docs/document133/.

58 See e.g. the explanation by the head of US Cyber Command, General Nakasone: Paul M. Nakasone and Michael Sulmeyer, 'How to Compete in Cyberspace', *Foreign Affairs*, 25 August 2020, available at https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

Cyber due diligence in practice

Japan's strategy, 'Proactive Cyber Defense' is centred around preventive or pre-emptive measures to counter *domestic* cyber threats, such as threat information and induced attacks.[59] This strategy seems to give effect not only to Japan's own constitutional legal framework, but also its international obligations not to allow its territory to be used for acts harmful to other states, as well as to protect the human rights of individuals within its jurisdiction.[60]

In the US, this doctrine is known as 'Defend Forward'[61] and its implementation relies on 'persistent engagement'[62] against *foreign* cyber threats. While this strategy has not been officially linked to any particular rule of international law, some scholars have opined that it has been or at least could be employed as a countermeasure against breaches of due diligence duties owed by third states — those failing to prevent malicious cyber operations emanating from their territory.[63] But this view cannot be easily reconciled with three key tenets of the law of state responsibility: a) that countermeasures must be directed against the state in breach, as opposed to non-state groups or individuals;[64] b) that states must notify and call upon the state in breach to comply with their obligations, except in the case of urgent countermeasures against imminent threats[65] (which, by definition, is not the case of pre-emptive operations); and, most importantly, c) that, for due diligence obligations to be breached, the harm or event to be prevented must have occurred.[66]

59 Cybersecurity Strategy 2018, *supra* note 50, at 22-23, 28.

60 Ibid, at 10, 35, 38-39.

61 2018 DoD Cyber Strategy, *supra* note 56, at 1, 2 and 7; US Cyber Command, 'Achieve and Maintain Cyberspace Superiority — Command Vision for US Cyber Command', 20 April 2018, available at https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf, at 4 and 6.

62 US Department of Defense, 'DoD General Counsel Remarks at U.S. Cyber Command Legal Conference', 2 March 2020, available at https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

63 Eric Talbot Jensen and Sean Watts, 'A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?', 95 *Texas Law Review* (2017) 1555, at 1555-1556, 1568.

64 Art. 49(1), ILC, Articles on Responsibility of States for Internationally Wrongful Acts, UNGA Res. 56/83, 12 December 2000 ('ARSIWA').

65 Art. 52(1)(a)(b), ibid.

66 Art. 14(c), ibid.

Cyber due diligence in practice

In the UK, a similar strategy to counter internal and external cyber threats has been framed as 'Active Cyber Defence',[67] and it has been explicitly linked to para 13(c) of the 2015 GGE Norms of Responsible State behaviour, i.e. the 'due diligence norm' mentioned earlier.[68] The connection suggests that active cyber defence is a means to fulfil the UK's own cyber due diligence obligations or responsibilities. Although this is a more plausible interpretation of such interventionist cyber strategies, it remains questionable whether those measures are consistent with other rules of international law, such as sovereignty, non-intervention and human rights.

Beyond general or military cyber strategies, most of states surveyed have adopted legislation specifying a range of technical, institutional, capacity-building and cooperative measures to be adopted primarily by executive bodies at different administrative levels. Prominent among these are China's Cybersecurity Law[69] as well as Russia's Federal Laws on: a) Information Technologies and Information Protection;[70] and b) the Security of Critical Information Infrastructure.[71] China's Cybersecurity Law is remarkably detailed and comprehensive, offering one of the broadest ranges of protection among all legal frameworks surveyed. It imposes on network operators 'security protection',[72] as well as emergency response and data back-up duties,[73] while tasking state bodies with the adoption of network standards, cyber education campaigns, network monitoring, periodic reporting, network security risk assessments and emergency response efforts.[74] For its part, Russia's Federal Laws provide strong protection for 'information contained within state information systems and also other data and

67 UK National Cyber Security Strategy', *supra* note 56, at 18, 33-69.

68 UK Non-Paper, *supra* note 167, at 6.

69 Cybersecurity Law (China), *supra* note 46.

70 Federal Law N. 276-FZ, *supra* note 46.

71 Federal Law N. 187-FZ, *supra* note 46.

72 Art. 25, Cybersecurity Law (China), *supra* note 46.

73 Art. 21, ibid.

74 Arts 15, 19, 51 and 53, ibid.

documents available at the disposal of state bodies'. Such protection is achieved through legal, organisational and technical measures safeguarding the confidentiality, availability and integrity of data from *any* illegal action, as well as the imposition of a range of preventive duties on information-holders, particularly network monitoring and threat detection.[75] Indeed, to effectively discharge their due diligence obligations in cyberspace, states must impose technical and administrative obligations on infrastructure, network and software operators, such as internet providers, webservers, encryption services, and telecom companies.[76]

b. Technical and Procedural Measures

While legal measures set abstract prescriptions and prohibitions, technical and procedural ones do the actual work of preventing, halting and mitigating the effects of harmful cyber operations in concrete situations. In this sense, compliance with due diligence obligations in cyberspace depends, to a large extent, on technical and procedural measures. A vast array of measures makes up this category, but key examples include accreditation schemes, protocols and standards, monitoring, encryption, access control, and firewalls. As ICTs evolve, more and more technical measures will likely be added to this list. There is much debate as to whether existing technologies can effectively *prevent*, as opposed to simply halt or respond to, imminent or forthcoming cyberattacks, especially in transit states.[77] Reasons include the high speed and complex routing of data packets on the internet, coupled with the employment of spoofing techniques, such as VPNs, internet anonymity and social engineering or deception methods, which make it increasingly difficult to identify, track and trace malware

75 Art 16, Federal Law N. 149-FZ, *supra* note 46.

76 See ITU GCA Report, *supra* note 9, at 7, para 1.9a.

77 Schmitt, *Tallinn Manual 2.0 supra* note 6, at 45, para 8. See also Eneno O. 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 215; Rebecca Crootof, 'International Cybertorts: Expanding State Accountability in Cyberspace', 103 *Cornell Law Review* (2018) 565, at 611, Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View – Future Challenges Essay* (2011), available at https://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf, at 9-10.

Cyber due diligence in practice

and other types of malicious cyber activity.[78]

There is also some reluctance among legal scholars and some states to accept network monitoring as a technical due diligence measure, in light of privacy concerns.[79] However, these concerns are grounded in misconceptions about the content of due diligence duties and the nature of technology itself. On the one hand, due diligence obligations are limited by each state's knowledge of particular malicious cyberoperations, whether these are imminent or still distant in time, as well as their capacity to act in the circumstances, including their technical know-how.[80] Thus, states that still do not possess the necessary technology to prevent malicious cyber operations are not required to do so, but must only mitigate or redress their impact, as far as possible. Although the details of the most sophisticated cybersecurity technologies employed by states to prevent cyber harms are not in the public domain, at least China,[81] Russia,[82] South Africa,[83]

78 See generally Charles R. Severance, *Introduction to Networking: How the Internet Works* (Creative Commons, 2015), at 6, 37-45. For an example of such difficulties, see Tomohiro Mikanagi and Kubo Mačak, 'Attribution of cyber operations: an international law perspective on the Park Jin Hyok case', 9 *Cambridge International Law Journal* (2020) 51, at 56-59.

79 Schmitt, *Tallinn Manual 2.0*, *supra* note 6, at 44-45, paras 7 and 10; Irène Couzigou, 'Securing cyber space: the obligation of States to prevent harmful international cyber operations', 32 *International Review of Law, Computers & Technology* (2018), at 50-51; Okwori, *supra* note 77, at 215; Jensen and Watts, *supra* note 63, at 1566; Akiko Takano, 'Due Diligence Obligations and Transboundary Environmental Harm: Cybersecurity Applications', *36 Laws* (2018) 7, at 8. Among states, see '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', 29 May 2020, available at https://www.dfat.gov.au/sites/default/files/submission-by-australias-representative-to-the-gge-norm-implementation-may-2020.pdf ('Australia's GGE Submission'), at 4-5 (referring to norm 3 of the Norms of Responsible State Behaviour); Canada's Proposals on OEWG pre-draft', *supra* note 36, 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)', April 2020, available at https://front.un-arm.org/wp-content/uploads/2020/04/ecuador-comments-on-initial-pre-draft-oewg.pdf.

80 See Coco and de Souza Dias, *supra* note15, at 5.

81 Arts 21(3) and 51, Cybersecurity Law (China), *supra* note 46.

82 Art 4(6), Federal Law N. 276-FZ, *supra* note 46; Law N. 187-FZ, *supra* note 46; New Strategy for Development of Information Society, *supra* note 50.

83 National Cybersecurity Policy Framework (South Africa), *supra* note 52, s. 7(c).

Cyber due diligence in practice

Japan,[84] the UK,[85] the US,[86] and France[87] have already indicated that such preventive techniques have been employed and are part and parcel of their national cyber security strategies. On the other hand, monitoring is not to be conflated with digital surveillance: while the latter refers to the focussed or targeted seeking of data in digital systems,[88] the former is the continual and passive scanning of networks or systems for malicious operations fitting certain parameters, showcasing a certain 'signature' or presenting unusual behaviour.[89]

Among the states surveyed, some technical measures seem to be more popular than others. In particular, technical standards, verification, certification or accreditation schemes are listed in legal or policy documents issued by China,[90] Japan,[91] the UK,[92] Germany,[93]

84 Cybersecurity Strategy 2018, *supra* note 53, at 27-29, 31, 35.

85 The Network and Information Systems Regulations 2018, supra note 46, Part II, s. 5(2)(a); Joint Doctrine Note 1/18: Cyber and Electromagnetic Activities, 21 February 2018, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf, para 4.3.

86 Ss. 12-13, Cybersecurity Information Sharing Act of 2015 (CISA) (Title I of the Cybersecurity Act of 2015) (6 U.S.C. §§ 1501-1510), available at https://uscode.house.gov/view.xhtml?req=(title:6%20section:1501%20edition:prelim); US Department of Homeland Security Cybersecurity Strategy, 15 May 2018, available at https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf, at A-2.

87 National Digital Security Strategy, *supra* note 50.

88 Global Information Society Watch, 'Communications surveillance in the digital age', 2004, available at https://giswatch.org/sites/default/files/digital_surveillance.pdf, at 19.

89 UK National Cyber Security Centre, '10 steps to cyber security: Monitoring', available at https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/monitoring. In this respect, it is interesting to note how, in the US Cyber Command practice, monitoring of military networks has been carried out according to a 'zero-trust' policy, according to which every host, server and connection is treated as potentially hostile. See Nakasone and Sulmeyer, *supra* note 58.

90 China's Ministry of Foreign Affairs, Global Initiative on Data Security, 8 September 2020, available at https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1812951.shtml; National Cyberspace Security Strategy, Principle IV, 3; Arts 15 and 17, available at https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/; Cybersecurity Law (China), *supra* note 46.

91 Cybersecurity Strategy 2018 (Japan), *supra* note 50, at 20-21, 23, 27, 38.

92 UK Non-Paper, *supra* note 35, at 14; The Network and Information Systems Regulations 2018, *supra* note 46, Part II, s. 5(2)(g); National Security Strategy and Strategic Defence and Security Review 2015, para 4.110, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf.

93 Act on the Federal Office for Information Security (BSI Act – BSIG), 14 August 2009, s. 3, paras 4-6, available at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf?__blob=publicationFile&v=4; IT Security Act (IT-Sicherheitsgesetz: Gesetz zur Erhörung der Sicherheit informationstechnischer Systeme), 17 July 2017, available at https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf.

Cyber due diligence in practice

South Africa,[94] and Brazil.[95] According to the technical experts who participated in the ITU's Global Cybersecurity Agenda, transparent, interoperable and non-discriminatory global standards for ICTs, which could build on existing frameworks such as ISO/IEC JTC 1/ SC 27, IT Baseline Protection Manual, COBIT and ITU-T X-series Recommendations, are instrumental in ensuring baseline security for ICT products, including hardware, firmware and software.[96] Robust cybersecurity protocols that follow accepted international standards can not only prevent harmful intrusions, but also effectively mitigate and remedy any ensuing consequences.[97] In particular, as both China[98] and the UK[99] have recently highlighted, technical standards are an effective means to protect the integrity of ICT supply chains and prevent hidden functions, such as malware installed in products through the backdoor, in line with the norm of responsible state behaviour articulated in para 13(i) of the 2015 GGE Report. Technical standards and certification schemes have also been endorsed as a technical due diligence measure by G7[100] members, as well as several prominent NGOs operating in the field, such as the ICRC, Global Partners Digital, Institute for International Cyber Stability and the International Cyber Policy Centre.[101]

Other popular technical and procedural measures, adopted by sampled states, include: a) cryptography or encryption, to protect access

94 National Cybersecurity Policy Framework, *supra* note 52, s. 7(h); Electronic Communications and Transactions Act No. 25, *supra* note 47, s. 55.

95 National Cybersecurity Strategy (E-Ciber), *supra* note 51, para 2.3.1.

96 ITU GCA Report, *supra* note 9, paras 2.7, 2.10. See also Scott J. Shackelford, J.D., Scott Russell, J.D., and Andreas Kuehn, 'Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors', 17 *Chicago Journal of International Law* (2016) 1 (proposing to implement cyber due diligence by drawing lessons from private technical standards).

97 Cyber Watching, 'Relevant Standards for Cybersecurity Risk Management', available at https://cyberwatching.eu/relevant-standards-cybersecurity-risk-management.

98 Global Initiative on Data Security, *supra* note 90.

99 UK Non-Paper, *supra* note 167, at 13-14.

100 G7, 'Cyber Norm Initiative: Synthesis of Lessons Learned and Best Practices', 26 August 2019, available at https://www.diplomatie.gouv.fr/IMG/pdf/_eng_synthesis_cyber_norm_initiative_cle44136e.pdf, at 2.

101 Australia's Public Consultation, *supra* note 18, at 2, 5, 8, 10, 15.

Cyber due diligence in practice

to confidential information and systems;[102] b) cybersecurity risk assessments, prepared on the basis of information reported on previous incidents and new threats;[103] c) vulnerability disclosure programmes, to ensure the safety of technical experts who spot errors and security vulnerabilities in software;[104] d) cyber threat reports, to allow individuals and businesses to understand the cyber threat landscape and prepare against them;[105] e) incident categorisation, to mobilise the right human, technical and financial resources;[106] f) drills or exercises, to prepare cybersecurity teams in the event of a cyber emergency;[107] g) testing and verification of software and hardware, to spot, identify, prevent and correct errors in code or assemblage that lead to system failure or security vulnerabilities;[108] and h) blockchain, to create

102 National Cybersecurity Strategy (E-Ciber) (Brazil), *supra* note 51, para 2.3.1., 2.3.3., 2.3.7; Art. 21(4), Cybersecurity Law (China), *supra* note 46; s. 3(8), BSI Act – BSIG (Germany), *supra* note 93; New Strategy for Development of Information Society (Russia) *supra* note 50; s. 9, National Cybersecurity Policy Framework (South Africa), *supra* note 52; UK National Cyber Security Strategy' *supra* note 56, paras 3.8 and 6.6.

103 Art. 17, 26 and 53, Cybersecurity Law (China), *supra* note 46; ss. 3(2), 8a(3), 8c(1), BSI Act – BSIG (Germany), *supra* note 93; ss. 5.4.5, 5.4.8, 6.3.6.7, National Cybersecurity Policy Framework (South Africa), *supra* note 52; UK National Cyber Security Strategy, *supra* note 56, para 7.4.

104 See OEWG, 'Final Substantive Report', 10 March 2021, UN Doc. A/AC.290/2021/CRP.2 ('OEWG Final Substantive Report'), para 28; 'Vulnerabilities Equities Policy and Process for the United States Government', 15 November 2017, available at http://d-russia.ru/wp-content/uploads/2017/11/VEP-Charter.pdf; Sue Helpern, 'After the SolarWinds Hack, We Have No Idea What Cyber Dangers We Face', *The New Yorker*, 25 January 2021, available at https://www.newyorker.com/news/daily-comment/after-the-solarwinds-hack-we-have-no-idea-what-cyber-dangers-we-face. See also Australia's Public Consultation, *supra* note 18 at 6, 10-17; G7, *supra* note 100 at 3.

105 E.g., Australian Cyber Security Centre, 'ACSC Annual Cyber Threat Report July 2019 to June 2020', available at https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf; UK National Cyber Security Centre, 'Weekly threat reports', available at https://www.ncsc.gov.uk/section/keep-up-to-date/threat-reports?q=&defaultTypes=report&sort=date%2Bdesc; 'Singapore Cyber Landscape 2019', 26 June 2020, available at https://www.csa.gov.sg/news/publications/singapore-cyber-landscape-2019. See also Australia's Public Consultation, *supra* note 18, at 3, 10-11, 15.

106 UK National Cyber Security Centre, 'New Cyber Attack categorisation system to improve UK response to incidents', 11 April 2018; available at https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents; Australian Government, 'Cyber Incident Management Arrangements for Australian Governments', March 2019, available at https://www.cyber.gov.au/sites/default/files/2019-03/cima_2018_A4.pdf; US National Institute of Standards and Technology, 'Cybersecurity Framework', available at https://www.nist.gov/cyberframework. See also Australia's Public Consultation, *supra* note 18, at 3.

107 National Cybersecurity Strategy (E-Ciber) (Brazil), *supra* note 51, para 1.3; Arts 34(4), 39(2), 53, Cybersecurity Law (China), *supra* note 46, ss. 5.4.8, 6.3.6.7, National Cybersecurity Policy Framework (South Africa), *supra* note 52; UK National Cyber Security Strategy', *supra* note 56, paras 5.3.5, 5.4.6; Ministry of Defence of Japan, 'Defense of Japan: Annual White Paper', 2020, available at https://www.mod.go.jp/en/publ/w_paper/wp2020/pdf/index.html, at 272.

108 Cybersecurity Law (China), *supra* note 46, Arts 17, 26, 39(2), 62; s. 8c(2)-4, BSI Act – BSIG (Germany), *supra* note 93, ss. 5.4.5, 7; Cybersecurity Strategy 2018 (Japan), *supra* note 50, at 43; National Cybersecurity Policy Framework (South Africa), *supra* note 52; The Network and Information Systems Regulations 2018 (UK), *supra* note 46, s. 12(2)(c)(iv). To take a concrete example of how these measures work in practice, see the process of verification (*homologation*) which the French Ministry of Defence uses for the information systems it employs. The steps include mapping the system and the entities which will use it within the government and checking whether the system under verification has the ability to: adjust its security according to threats; monitor possible cyber attacks and capably react to them; ensure that a cyber attack does not spread inside the system and out to other ones; report the threat or attack and continue to work." (see Instruction N° 101000/ARM/CAB Relative à La Politique de Lutte Informatique et Défensive Du Ministère Des Armées Du 7 Février 2019, 7 February 2019 (France), para 1.6, available at https://www.legifrance.gouv.fr/circulaire/id/44356).

immutable online ledgers or records and secure the implementation of automated transactions.[109] These and other measures provide states with a comprehensive and flexible arsenal to fulfil their due diligence obligations under international law. Not only are they conducive to protecting states, businesses and individuals from cyber harm but also fostering trust in technology, building confidence among states, and thereby preventing trade wars, diplomatic crises and armed conflict.

c. Organisational Structures

Legal and technical measures, even if detailed and technologically advanced, are not necessarily effective if their implementation and execution is not properly coordinated at the various levels of governmental and private activity. Effective prevention, mitigation and remediation of harmful cyber operations depend, to a large extent, on the coordination and communication between the various actors involved in such preventive action and response, including both state and non-state entities. This view is reflected in the ITU's Global Cybersecurity Agenda, whose typology include 'organizational structures' as a third area where states are encouraged to behave diligently and adopt appropriate measures.[110] Thus, establishing a clear national organisational structure is an example of diligent behaviour which would allow states to comply with their international obligations. The creation of such structures can easily be read as an effort to prevent, respond to and mitigate the effects of harmful cyber operations.

It is possible identify at least two sets of organisational measures which states have adopted to ensure better governance of ICTs under their control or jurisdiction: on one side, the establishment of central governmental agencies or bodies, responsible for cyber-related matters (including response to computer emergencies or security incidents); on the other, the conclusion of public-private partnerships and platforms for multi-stakeholder collaboration.

109 National Cyber Security Strategy (Canada), *supra* note 49, at 24, 27-28; Cybersecurity Strategy 2018 (Japan), *supra* note 50, at 7, 17, 46.

110 ITU GCA Report, *supra* note 9, Section 3.

Cyber due diligence in practice

i. National Cybersecurity Structures

Starting with national cybersecurity structures, it has been relatively common for states to establish a central authority with strategic, regulatory and coordination powers. For instance, to better coordinate its cybersecurity policies, action and complex organisational structure,[111] France instituted in 2009 a National Cybersecurity Agency (*Agence nationale de la sécurité des systèmes d'information*, ANSSI),[112] with a threefold mission: i) coordinate the work of the various ministries and governmental entities on cybersecurity; ii) prescribe to these entities — in particular those with responsibility for critical infrastructure (*opérateurs d'importance vitale*, OIV) — the adoption of measures of preventive security and reaction to cyber attacks, whilst monitoring their implementation; as well as iii) coordinate national cyber defence and respond directly to attacks.[113] Similarly, by virtue of its 2014 Cybersecurity Basic Act,[114] Japan established a specialized body within its government: the Cyber Security Strategic Headquarters, which manage the country's cybersecurity strategy by identifying key security measures and preparing to respond to major cyber incidents. In 2015, Japan also established the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), as a secretariat for the Cyber Security Strategic Headquarters.[115] A number of special units where entrusted with continuously monitoring communication and information systems and with responding to cyber attacks, including for instance the Cyber Defense Group.[116] Similarly, the US' efforts to enhance the security of its cyber infrastructure have been informed, among other things, by the best practices and guidelines developed by the National Institute for Security and Technology's

111 Secrétariat général de la défense et de la sécurité nationale, 'Revue Stratégique de Cyberdéfense', 15 March 2018 (France), available at http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense, at 46–48.

112 Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information », 7 July 2009 (France), available at https://www.legifrance.gouv.fr/loda/id/JORFTEXT000020828212/.

113 Revue Stratégique de Cyberdéfense (France), *supra* note 111, at 46–47 and 108–111.

114 s 24ff, Basic Act on Cybersecurity 2014, (Japan) *supra* note 46.

115 See Government of Japan, 'National center of Incident readiness and Strategy for Cybersecurity (NISC)', available at https://www.nisc.go.jp/eng/ -sec1; Defense of Japan: Annual White Paper, *supra* note 107, at 270.

116 Ibid, at 271.

Cyber due diligence in practice

(NIST) in their 'Framework for Improving Critical Infrastructure Cybersecurity'.[117] All US federal agencies are required to manage their cybersecurity risks by implementing the Framework's guidelines, by virtue of a Presidential Executive Order.[118] And, in 2018, the US created a Cybersecurity and Infrastructure Security Agency (CISA), with the task to pursue capacity building and resilience against cyber attacks, offer cybersecurity and incident response services and in general support and coordinate the government's action in cyber matters.[119] Other sampled countries have also established or committed to establishing a national cyber authority, including Brazil,[120] Canada,[121] China,[122] Germany[123] and the UK.[124] The importance of setting up proper organisational structures can also be inferred from the requirement, under the EU Directive on the Security of Network and Information Systems ('NIS Directive'), to establish competent national authorities and Computer Security Incident Response Teams (CSIRTs).[125]

A military cyber command structure, hinging on the Ministry of Defence (or equivalent), is also quite common across different states.[126]

117 NIST, 'Framework for Improving Critical Infrastructure Cybersecurity 1.1', 16 April 2018, available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

118 President of the US, Executive Order 13800, 'Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure', 11 May 2017, available at https://www.govinfo.gov/app/details/DCPD-201700327, para 1(c)(ii).

119 Cybersecurity and Infrastructure Security Agency Act of 2018 (US). See also https://www.cisa.gov/about-cisa.

120 Art. 2.3.2, National Cybersecurity Strategy (E-Ciber) (Brazil), *supra* note 51.

121 National Cyber Security Strategy (Canada), *supra* note 49, explaining the institution of a new Canadian Centre for Cyber Security, at III.

122 Art. 25, 2015 National Security Law of the People's Republic of China, 01 July 2015, available at https://www.chinalawtranslate.com/2015nsl/?lang=en/.

123 BSI Act – BSIG (Germany), *supra* note 93, in particular s. 3.

124 In 2016 the UK created the National Cyber Security Centre (more information available at https://www.ncsc.gov.uk/). And among other instruments, the Network and Information Systems Regulations 2018, 10 May 2018 (available at https://www.legislation.gov.uk/uksi/2018/506/made), *inter alia* designated GCHQ as CSIRT for the country. See also UK Non-Paper, *supra* note 167, detailing the activities of the National Cyber Security Centre and other central bodies.

125 Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (EU), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148.

126 E.g., General Directorate of Cyberdefense (Dirección General de Ciberdefensia), Ministry of Defense (Argentina), available at http://www.fuerzas-armadas.mil.ar/Dependencias-CIBDEF.aspx; Information Warfare Division, Department of Defence (Australia), available at https://www.defence.gov.au/jcg/iwd.asp; Cyber Defense Command (Comando de Defesa Cibernética), Ministry of Defense (Brazil), available at https://dialogo-americas.com/

Cyber due diligence in practice

For instance, when it comes to military matters and the protection of national networks from foreign attacks, the US cyber strategies and policies are determined by a central Cyber Command, created in 2010 after a hostile cyber operation had hit, in 2008, the US Department of Defense's classified and unclassified networks from foreign attacks.[127] The results of the US Cyber Command's activities are shared with other domestic bodies at the federal, state and local level, in particular with the National Security Agency and the Federal Bureau of Investigation,[128] in an instructive example of how open communication channels between the various branches of government can effectively address cyber threats. Similarly, French cybersecurity depends partly on the activities of the Ministry of Defence (*Ministère des Armèes*) and of its Cyber Command (*ComCyber*).[129] Such activities are pursued within an elaborate organizational and regulatory framework which was lastly detailed in 2018.[130] As part of this framework, the *Centre d'analyse en lutte informatique defensive* (CALID) — operating 24/7 and placed under the authority of ComCyber — keeps track of all known vulnerabilities and, in case of attack against the Ministry's networks, acts as Computer Emergency Response Team (CERT).[131] France also offers a good example of organizational measures adopted not only to strategize and coordinate action in cyber matters, but also to facilitate specialised criminal investigations and prosecutions of those responsible for harmful cyber operations and other forms of cyber crime. These efforts have resulted in the establishment of a specialized cyber criminality section within

articles/brazilian-army-invests-in-cyber-defense/; Strategic Support Force (SSF) of the People's Liberation Army (PLA) (China), available at http://www.mod.gov.cn/power/node_47605.htm; National Cyberdefence Center (Nationales Cyber-Abwehrzentrum) (Germany), available at https://www.bka.de/DE/UnsereAufgaben/Kooperationen/NCAZ/ncaz_node.html; Cyber Defense Command (Iran), available at https://www.papsa.ir/; Ministry of Defence and Self-Defense Forces (Japan), 'Regarding Response to a Cyber Attack', available at https://www.mod.go.jp/en/publ/answers/cyber/index.html#a2; Defence Cyber Organisation, Ministry of Defence and Singapore Armed Forces (Singapore), available at https://www.mindef.gov.sg/web/portal/mindef/defence-matters/defence-topic/defence-topic-detail/cyber-defence; Cyber Regiment, Ministry of Defence (UK), available at https://www.gov.uk/government/news/armed-forces-announce-launch-of-first-cyber-regiment-in-major-modernisation.

127 Nakasone and Sulmeyer, *supra* note 58.

128 Ibid.

129 Art. D 3121-14-1, Code de la Defense (France), 13 December 2019, available at https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006071307.

130 'Instruction N° 101000/ARM/CAB Relative à La Politique de Lutte Informatique et Défensive Du Ministère Des Armées Du 7 Février 2019', 7 February 2019, (France), available at https://www.legifrance.gouv.fr/circulaire/id/44356.

131 Ibid, paras 2.3.1.3.

Cyber due diligence in practice

the Paris Prosecutor Office and in the allocation to the Paris Court of First Instance of centralized jurisdiction over ICT attacks.[132]

ii. Public-Private Partnerships

Considering that the majority of online activities is carried out, controlled or overseen by private entities, a good faith engagement and open dialogue between states and the private sector is indispensable to prevent, stop and respond to harmful cyber operations.[133] Thus, public-private partnerships feature heavily in the legal frameworks or cyber policy strategies of several states surveyed.[134] For example, the US have indicated several times in their 2018 National Cyber Strategy how much they value public-private partnerships to enhance cybersecurity.[135] Operationalizing the cybersecurity collaboration between the public and the private sector is also one of the pillars of the recommendations for reform proposed by the US Cyberspace Solarium Commission.[136] In the same vein, in its 2018 Strategic Review of Cyberdefence, France noted how the objective of national cybersecurity cannot be achieved without involving the private sector

132 Revue Stratégique de Cyberdéfense (France), *supra* note 111, at 72; 'Stratégie Internationale de La France Pour Le Numérique', 22 May 2019 (France), available at https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/la-strategie-internationale-de-la-france-pour-le-numerique/, at 13. See also Art. 706-772ff., French Code of Criminal Procedure, introduced by Law n ° 2016-731 of June 3, 2016, available at https://www.ojp.gov/ncjrs/virtual-library/abstracts/french-code-criminal-procedure-revised-edition. In the same vein, see National Cyber Security Strategy (Canada), *supra* note 49, explaining the institution of a National Cybercrime Coordination Unit, at III; and UK Non-Paper, *supra* note 35, describing the work of the National Cyber Crime Unit.

133 See Smith, *supra* note 25, noting that '[u]nlike attacks from the past, cybersecurity threats also require a unique level of collaboration between the public and private sectors. Today's technology infrastructure, from data centers to fiberoptic cables, is most often owned and operated by private companies. These represent not only much of the infrastructure that needs to be secured but the surface area where new cyberattacks typically are first spotted. For this reason, effective cyber-defense requires not just a coalition of the world's democracies, but a coalition with leading tech companies.'

134 E.g., Russian National Security Strategy, December 2015, available at http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf, para 69; Statement by David Koh, Chief Executive of the Cybersecurity Agency of Singapore during UNSC Arria Formula Meeting on Cybersecurity, 22 May 2020, available at https://www.youtube.com/watch?v=CbBchZEG5D8, timestamp 25:00; s. 7(e), National Cybersecurity Policy Framework, *supra* note 52; The Network and Information Systems Regulations 2018 (UK), *supra* note 46, Part II, s. 5(c); National Cybersecurity Strategy (Argentina), *supra* note 53, National Cybersecurity Strategy (E-Ciber) (Brazil), *supra* note 51, paras 2.3.2-2.3.3; National Cyber Security Strategy (Canada), *supra* note 49, para II. See also OEWG, 'Chair's Summary', 10 March 2021, UN Doc. A/AC.290/2021/CRP.3, paras 28, 36 and 45.

135 'National Cyber Strategy of the United States of America', September 2018, available at https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf, at 8-10, 14-15, 17 and 25, for e.g..

136 US Cyberspace Solarium Commission, 'Final Report', March 2020, available at https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view, at 5.

Cyber due diligence in practice

and imposing on them certain security standards.[137]

States have implemented partnerships with the private sector through a number of measures, the most notable of which includes setting up permanent bodies to facilitate continuous dialogue and joint initiatives. Australia has been particularly active in this respect. Since 2003, it has operated a mechanism known as the Trusted Information Sharing Network for Critical Infrastructure Resilience, a forum for information-sharing between businesses and government with respect to risks and vulnerabilities of critical infrastructure, aimed at enhancing its security and resilience.[138] In 2019, the Australian Government also established an Industry Advisory Panel, to foster dialogue between the public and the private sector and make recommendations as to how the two different sectors can operate to achieve better security.[139] In addition, Australia decided to invest in the development of several Joint Cyber Security Centres (JCSCs) across its territory, as collaborative outlets to enhance cyber security practices.[140]

Australia has not been the only country engaging in an institutionalised collaboration with the private sector. For instance, in line with the multi-stakeholder approach set forth in its national law[141] and espoused in its Cybersecurity Strategy,[142] Japan has instituted a Cyber Defense Council, comprising industry representatives from the defence sector with interest in cyber matters.[143] On its part, the US government has notably encouraged the development of private Information Sharing

137 Revue Stratégique de Cyberdéfense (France), *supra* note 111, at 87–91.

138 Australian Government, 'Trusted Information Sharing Network for Critical Infrastructure Resilience (TISN)', available at https://cicentre.gov.au/tisn. See also DFAT, 'Australian Implementation of Norms of Responsible State Behaviour', May 2020, available at https://www.dfat.gov.au/sites/default/files/how-australia-implements-the-ungge-norms.pdf, at 10.

139 Australian Government, 'Australia's Cyber Security Strategy 2020', available at https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf, at 16, paras 21-23. After the Panel concluded its work, Australia committed to replacing it by a standing Industry Advisory Committee. Ibid., at 16, para 24.

140 Ibid, at 23, para 38-39.

141 Basic Act on Cybersecurity 2014, (Japan) *supra* note 46.

142 Japan, 'Cybersecurity Strategy', 27 July 2018, available at https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf, at 3 and 33ff.

143 Defense of Japan: Annual White Paper, *supra* note 57, at 272.

Cyber due diligence in practice

and Analysis Organizations (ISAOs),[144] i.e. groups 'created to gather, analyze, and disseminate cyber threat information',[145] whose activities are coordinated by a central ISAO Standards Organization.[146] And as a complement to such efforts, the US Cyber Command has also created near its headquarters a facility known as 'DreamPort', which hosts dialogues between public and private partners and employs interns from nearby schools.[147] Collaboration with the private sector has been at the heart of the EU's cybersecurity strategy, too. In 2016, the European Commission entered a so-called 'contractual public-private partnership' (cPPP) with the European Cybersecurity Organisation (ECSO), a private organisation founded for this purpose under Belgian law.[148] The objectives of this partnership include increased cooperation between governments and the industry resulting in more secure and human rights-compliant ICT products, services and software; and helping the industry sector in Europe to achieve better cybersecurity.[149]

Information sharing and public-private collaboration could also be carried out in a less institutionalised manner, as exemplified by US practice. Even though controversial for its privacy repercussions, the 2015 US Cybersecurity Information Sharing Act (CISA) has facilitated the exchange of Internet-traffic and other personal information between private entities and the US government, with respect to cyber threats, cyber incidents or the prevention, investigation and prosecution of cybercrime, as well as other forms of criminality.[150]

144 US President, Executive Order 13691, 'Promoting Private Sector Cybersecurity Information Sharing', 13 February 2015, available at https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

145 CISA, 'Frequently Asked Questions', available at https://www.cisa.gov/information-sharing-and-analysis-organizations-isaos.

146 The ISAO Standards Organization is currently an NGO based at the University of Texas at San Antonio, supported by the Logistics Management Institute (LMI) and the Retail Cyber Intelligence Sharing Center (R-CISC). See ibid.

147 Nakasone and Sulmeyer, *supra* note 58.

148 See ECSO, 'About', available at https://ecs-org.eu/about.

149 See ECSO, 'contractual Public-Private Partnership (cPPP) with the European Commission', available at https://ecs-org.eu/cppp.

150 US Congress, Cybersecurity Information Sharing Act, S. 2588 (Pub. L. No. 114-113), 18 December 2015, available at https://www.cisecurity.org/newsletter/cybersecurity-information-sharing-act-of-2015/. See in particular Section 104(c)(1). See also Brad S. Karp, Paul, Weiss, Rifkind, Wharton & Garrison LLP, 'Federal Guidance on the Cybersecurity Information Sharing Act of 2015', 3 March 2016, available at https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/.

Cyber due diligence in practice

In addition, it appears also that the results of US Cyber Command's 'defend forward' operations have been publicly released and/or shared with industry operators, especially antivirus companies, in order to increase security for their users.[151]

Finally, in an effort to solicit advice and suggestions from the industry, civil society and other stakeholders, in 2019, Australia has published a 'call for views'[152] about how to improve its national cybersecurity.[153] Such consultations eventually contributed to inform the 2020 Australian Cyber Security Strategy.

In sum, organisational measures enable the establishment of clearly defined competences, reliable communication and coordination channels among different government sectors, institutionalised sharing of expertise between public and private entities. Their *fil rouge* is to undoubtedly favour preparedness in the face of cyber incidents, thereby fostering diligent behaviour in cyberspace.

d. Capacity Building

Duties to act with due diligence are often described as 'best efforts' obligations requiring 'all feasible measures' in the circumstances. Consequently, one of their essential ingredients is the duty-bearer's capacity to act diligently. However, the state practice surveyed evinces a dynamic understanding of this element: building (or acquiring) more and more capacity to prevent, respond to and mitigate the effects of harmful cyber operations is in itself a way of exercising 'best efforts',

151 Nakasone and Sulmeyer, *supra* note 58. In fact, it is interesting to note that, in a 2016 Presidential Policy Directive, the US committed to respond to cyber incidents by, inter alia, "*furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents; identifying other entities that may be at risk and assessing their risk to the same or similar vulnerabilities; assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks; facilitating information sharing and operational coordination with threat response; and providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery.*" US Presidential Policy Directive/PPD-41, 'United States Cyber Incident Coordination', 26 July 2016, para IV(b), available at https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

152 Australian Government, 'Australia's 2020 Cyber Security Strategy: A call for views', 2019, available at https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-strategy-2020-discussion-paper.pdf.

153 Australia's Cyber Security Strategy 2020, *supra* note 139, at 15, paras 17-19. See also Australian Government, 'Discussion paper - 2020 Cyber Security Strategy', 2020, available at https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-strategy-2020.

Cyber due diligence in practice

or one of the 'feasible measures' which states can adopt to discharge their due diligence obligations. An obligation (of result) to put in place the minimum capacity also underlies, as a separate component, the due diligence obligations mentioned earlier. This means that lack of capacity at a given moment in time is no excuse for inaction. Likewise, a state may well be in breach of its due diligence obligations (of conduct) when, having the ability to do so, it failed to acquire the capacity to prevent, respond to or mitigate certain cyber operations. Thus, at least the basic technical and administrative apparatus to cope with cyber incidents must be set up. Moreover, whenever a state has the capacity to acquire additional means to prevent, stop or mitigate cyber harms, it must 'upgrade' and 'update' its own capacity as far as possible. The more capacity a state will be able to build, the more it is expected to. Therefore, capacity-building as a way to behave diligently implicates embarking on a continuous path of research and education. Most states surveyed take cyber capacity-building very seriously, along at least two strands: i) training of a capable 'cyber' workforce, including in technical, legal and policy areas;[154] and ii) public awareness campaigns to build a culture of cybersecurity across the population.[155]

Some countries have adopted broad initiatives in this sense. A paradigm example is the 10-year programme of investment and capacity-building known as 'Cyber Enhanced Situational Awareness and Response (CESAR) package', launched by Australia in June 2020.[156] The measures included in the package aim, inter alia: to strengthen the capacity to deal with cybercrime offshore, by supporting law enforcement agencies; to create a 'new cyber threat sharing platform' allowing private and public agents to share information about malicious cyber activity; to support telecommunication providers in achieving better cybersecurity related to their networks and services; to invest into research and development of intelligence capabilities;

154 See OEWG Final Substantive Report, *supra* note 104, paras 59-61.

155 Ibid, para 73.

156 Department of Defence of Australia, 'Nation's Largest Ever Investment in Cyber Security', 30 June 2020, available at https://www.minister.defence.gov.au/minister/lreynolds/media-releases/nations-largest-ever-investment-cyber-security. See also Brandon Kirk Williams, 'An Opportunity for Strengthening U.S.-Australian Cyber Cooperation', *Lawfare*, 16 September 2020, available at https://www.lawfareblog.com/opportunity-strengthening-us-australian-cyber-cooperation.

Cyber due diligence in practice

to disseminate cybersecurity guidelines and provide assistance to vulnerable sectors of the economy; to expand Australian cybersecurity workforce.[157] This last aim will be pursued through a Cyber Security National Workforce Growth Program, which will involve also academia and the private sector.[158] The growth of a capable and competitive cyber workforce has been a centrepiece in the practice of other countries as well. A 2017 US Presidential Executive Order identified it as one of the key components of the US action to improve the cybersecurity of its critical infrastructure,[159] in line with the stance of the US National Cyber Strategy on this issue.[160] Thus, to retain and recruit talent which often ends up joining the more remunerative private sector, the US Cyber Command has offered cyber personnel continuing opportunities for professional development, competitive salaries and attractive retirement or social security schemes.[161] Somewhat similarly, Japan's Defense Forces have launched a series of initiatives aimed at enhancing their personnel's cybersecurity expertise, including, inter alia: creating a common cyber course; encouraging personnel attendance at educational opportunities in foreign universities and institutions; setting aside funds to recruit talented individuals from the private sector.[162]

Along with these efforts, states have also sought to provide guidance to the existing workforce about how to prevent and respond to cyber incidents, enhancing their ability to do so effectively. Australia has published a number of documents containing cybersecurity advice for both the public and the private sector, most notably an Information Security Manual for the Australian government[163] and a document

157 Department of Defence of Australia, ibid. See generally Australia's Cyber Security Strategy 2020, *supra* note 139.

158 Australia's Cyber Security Strategy 2020, *supra* note 139, at 33.

159 US Executive Order 13800, *supra* note 118, para 3(d).

160 National Cyber Strategy of the United States of America, *supra* note 135, at 17. See also US Department of Homeland Security, 'Cybersecurity Strategy', 15 May 2018, available at https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf, Objective 6.4, at 24–25.

161 Nakasone and Sulmeyer, *supra* note 58. The Cyber Command, in doing so, has also partnered with institutions like the National Security Innovation Network.

162 Defense of Japan: Annual White Paper, *supra* note 107, at 272–273.

163 See Australian Government, 'Australian Government Information Security Manual (ISM)', available at https://www.cyber.gov.au/acsc/view-all-content/ism.

Cyber due diligence in practice

containing Strategies to Mitigate Cyber Security Incidents for private entities.[164] In 2017, Japan also issued a Cybersecurity Policy for Critical Infrastructure Protection, with five directives: maintenance and promotion of safety principles; enhancement of information sharing system; enhancement of incident response capability; risk management and preparation of incident readiness; and enhancement of the basis for critical infrastructure protection.[165] The idea behind the implementation of such policies is to guarantee that, in the event of a cyber incident, critical infrastructure and their managers have the necessary capabilities and resources to continue operating reliably.[166]

Educational measures aimed specifically at the broader population have been even more popular. In fact, the ITU experts concluded that more efforts are desirable, inter alia, 'in empowering end-users to adopt a safe behaviour in order to become responsible cyber-citizens; … [to] train and educate at several levels all the actors of the information society; … [and] …to develop human capacity in all aspects of cybersecurity to help build a global culture of cybersecurity.'[167] Relatedly, one of the stated aims of the EU NIS Directive is to build 'a culture of security across sectors which are vital for our economy and society and moreover rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.'[168] Notable among the sampled states is France, having recognised in its 2018 Strategic Review of Cyberdefence that it is not possible to achieve a satisfying national cybersecurity without implementing broad educational measures.[169] Education in cybersecurity, at least its building

164 Australian Cyber Security Centre, 'Strategies to Mitigate Cyber Security Incidents – Mitigation Details', February 2017, available at https://www.cyber.gov.au/sites/default/files/2020-06/PROTECT%20-%20Strategies%20to%20Mitigate%20Cyber%20Security%20Incidents%20%28February%202017%29.pdf. See also DFAT, 'Australian Implementation of Norms of Responsible State Behaviour', *supra* note 138, at 10–11.

165 Cybersecurity Strategy (Japan), *supra* note 50, at 24.

166 See also Japan, Cybersecurity Strategic Headquarters of Japan, 'Guideline for Establishing Safety Principles for Ensuring Information Security of Critical Infrastructure (5th Ed.)', 4 April 2018, available at https://www.nisc.go.jp/eng/pdf/principles_ci_eng_v5.pdf, at 1.

167 ITU GCA Report, *supra* note 9, paras 4.5-4.8.

168 European Commission, 'The Directive on security of network and information systems (NIS Directive)', 16 December 2020, available at https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

169 Revue Stratégique de Cyberdéfense (France), *supra* note 111, at 126–134. See also 'French National Digital Security Strategy', 16 October 2015, available at https://www.ssi.gouv.fr/en/actualite/the-french-national-digital-security-strategy-meeting-the-security-challenges-of-the-digital-world/, at 26–27.

Cyber due diligence in practice

blocks, should start from a young age and involve the whole public through general pedagogical initiatives, but also form cybersecurity experts with specialized programmes.[170] Among many initiatives, the French ANSSI conceived a MOOC ('Massive Online Open Course') on cybersecurity which is free to access.[171] Likewise, since 2006, Australia has operated the so-called 'Stay Smart Online' programme, providing advice to all citizens — especially home Internet users and small businesses — about good practices to protect themselves from online scams, malware and other cyber security threats.[172]

In the context of devising such educational and training opportunities, many countries paid particular attention to the need to build cyber threat-awareness among small and medium business enterprises.[173] For instance, Australia has vowed to provide cyber training to such entities, to establish a helpdesk for those who need assistance or advice, as well as to encourage bigger businesses to provide more comprehensive cyber security information and tools to small and medium businesses.[174] And the US have insisted on the crucial importance of creating awareness about digital supply chain threats[175] and cybersecurity best practices[176] for businesses, pledging to share intelligence about potential cyber threats with the relevant private entities.[177]

Whilst the examples discussed above are not always poised to make a difference in the short-term or in the immediacy of the response to a cyber attack, they undoubtedly trace a way for strengthening any state's ability to effectively discharge its own protective duties in cyber matters.

170 Revue Stratégique de Cyberdéfense (France), *supra* note 111, at 126–134.

171 See SecNumacadémie, 'Bienvenue sur le MOOC de l'ANSSI', available at https://secnumacademie.gouv.fr/.

172 See Australian Government, Australian Cyber Security Centre, 'Protect yourself against cybercrime', available at https://www.cyber.gov.au/acsc/view-all-content/sso/acscs-stay-smart-online-program.

173 Similarly, ITU GCA Report, *supra* note 9, paras 4.9-4.11.

174 Australia's Cyber Security Strategy, *supra* note 139, at 30, para 61.

175 National Cyber Strategy of the United States of America, *supra* note 135, at 7.

176 Ibid 25–26.

177 Among others. See US Presidential Policy Directive/PPD-41, *supra* note 151, para IV(c)-(d).

Cyber due diligence in practice

e. International Cooperation

As the Internet and other ICTs know no territorial boundaries, an open dialogue and good faith collaboration between states can go a long way in preventing harm and effectively responding to malicious cyber operations. As eloquently put by the 2015 GGE Report '[i]nternational cooperation and assistance can play an essential role in enabling States to secure ICTs and ensure their peaceful use.'[178] For instance, in line with the commitment adopted in its national law,[179] China has recently advocated that 'States should increase exchanges on standards and best practices with regard to critical infrastructure protection, and explore the possibilities to establish relevant risk early warning and information sharing mechanism [and] to improve protection capability for cyber security of states, especially developing countries, and promote emergency response and coordination in case of cyber attacks against critical infrastructure.'[180] And, as forcefully signalled by the US Deputy Secretary of State, '[w]e need all responsible states to stand together against destructive, disruptive, or otherwise destabling [sic], malicious cyber activity carried out by states during peacetime. *We must work in concert* to ensure that there are consequences for bad behavior in cyberspace, drawing upon all elements of national power, not just cyber

178 Ibid, para 19.

179 Art. 7, Cybersecurity Law (China), *supra* note 46: "*The State actively carries out international exchange and cooperation in the areas of cyberspace governance, research and development of network technologies, formulation of standards, attacking cybercrime and illegality, and other such areas; promoting the construction of a peaceful, secure, open and cooperative cyberspace; and establishing a network governance system that is multilateral, democratic and transparent.*"

180 China, 'Statement by Minister-Counsellor Mr. Yao Shaojun at Arria Formula Meeting on Cyber Attacks Against Critical Infrastructure', 26 August 2020, available at https://www.fmprc.gov.cn/ce/ceun/eng/hyyfy/t1809700.htm. See also China, 'Foreign Ministry Spokesperson Geng Shuang's Regular Press Conference on April 24, 2020', available at http://au.china-embassy.org/eng/fyrth/t1773113.htm.

Cyber due diligence in practice

capabilities. We need to build cooperation among responsible states to deliver those consequences where appropriate and consistent with international law.'[181] Commitments to international cooperation in the cyber field have also come from a number of other states.[182]

The question remains open as to whether international law imposes on states a self-standing duty to cooperate towards reaching certain aims — including but not limited to peace and security in cyberspace. Without prejudice to how such question should be answered, it seems plausible to frame international cooperation, at the very least, as one of the ways in which states may discharge their obligations to behave diligently in cyberspace. In this sense, France's position is instructive: under international law, a state from whose infrastructure a harmful cyber operation originates or transits cannot be said to behave diligently if it remains completely silent to requests of assistance by the victim state, or otherwise refuses to cooperate or put an end to the operation, when able to do so.[183] Rightly so, France believes international cooperation to be an essential component of cyber due diligence obligations, especially when it comes to the protection of critical infrastructure and response to major cyber attacks, including those transiting through third states.[184] Civil society groups have also expressed their support for this view.[185]

181 John Sullivan, US Deputy Secretary of State, 'Remarks at the Second Ministerial Meeting on Advancing Responsible State Behavior in Cyberspace', *United States Department of State*, 23 November 2019, available at https://www.state.gov/remarks-at-the-second-ministerial-meeting-on-advancing-responsible-state-behavior-in-cyberspace/, emphasis added. Of note, however, the Joint Statement on Advancing Responsible State Behaviour in Cyberspace, released by 26 countries (including the US) on the very same day of Deputy Secretary Sullivan's speech, uses much less strong language if one were looking for evidence of *opinio juris*: "*When necessary, we will work together on a voluntary basis* to hold states accountable when they act contrary to this framework, including by taking measures that are transparent and consistent with international law" (see 'Joint Statement on Advancing Responsible State Behavior in Cyberspace', *United States Department of State*, 23 November 2019, available at https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/, emphasis added).

182 See e.g. National Cyber Security Strategy, 2018 (Canada), *supra* note 49, at 31-32; BSI Act – BSIG (Germany), *supra* note 93, s. 3.16; UK Non-Paper, *supra* note 167, at 7-8; Arts 6, 19, 20, 34(2); Cybersecurity Law (China), *supra* note 46; National Cybersecurity Policy Framework (South Africa), *supra* note 52, ss. 1.2, 1.6, 2.7, 5.3.6, 6.4.3, 14, 18; National Cybersecurity Strategy (Argentina), *supra* note 53, Annex I, at 5; National Cybersecurity Strategy (E-Ciber) (Brazil), *supra* note 51, paras 2.2-2.4.

183 Revue Stratégique de Cyberdéfense (France), *supra* note 111, at 83–84.

184 Ibid 86. See also Stratégie Internationale de La France Pour Le Numérique (France), *supra* note 33, at 32.

185 See the submission by the Tech Accord and the Institute for International Cyber Stability in their responses to Australia's Public Consultation, *supra* note 18, at 12.

Cyber due diligence in practice

A survey of state practice reveals that cooperation, in this respect, may take different forms. An obvious one is the participation in international *fora* devoted to the study and clarification of rules, norms and best practices in the fields of information and communication technologies. The above mentioned GGE and OEWG, both created by the UN General Assembly, are but only two examples. The exchange of policy papers, position papers and suggestions for draft reports on these occasions represent a prolific way to share information and views, which are conducive to diligent or responsible state behaviour in cyberspace.[186]

However, in the face of specific harmful cyber operations, the sharing of information and expertise has at times assumed a more practical dimension. As a matter of fact, international cooperation may take the form of joint action to tackle cybercrime and other forms of malicious cyber operations, by means of sharing best practices and information, and carrying out joint operations. States have long insisted upon enhancing international collaboration with other states in order to prevent and respond to transnational cyber threats. For instance, in September 2020, the Five Eyes alliance — grouping the intelligence agencies of Australia, Canada, New Zealand, the UK and the US — released a joint advisory containing a so-called 'playbook' for responding to cyber incidents and carrying out effective investigations.[187] In addition, within the ASEAN Regional Forum (ARF), Australia and Malaysia have proposed the creation of an 'ARF Directory of Cyber Points of Contact', which facilitates communication between ARF members in case of cyber incidents with potential regional impact.[188] In the EU, the NIS Directive underlined the importance of international cooperation among all member States,

186 OEWG Final Substantive Report, *supra* note 104, paras 68-79.

187 CISA, 'Alert (AA20-245A), Technical Approaches to Uncovering and Remediating Malicious Activity', 24 September 2020, available at https://us-cert.cisa.gov/ncas/alerts/aa20-245a.

188 DFAT, 'Australian Implementation of Norms of Responsible State Behaviour', *supra* note 138, at 2. See also 'Draft Concept Paper, Australia-Malaysia, ASEAN Regional Forum (ARF) Directory of Cyber Points of Contact', March 2016, available at http://aseanregionalforum.asean.org/wp-content/uploads/2019/03/Annex-14-Concept-Paper-for-ARF-Directory-of-Cyber-Points-of-Contact-14th-ism-on-cttc.pdf. A number of other cooperation initiatives sponsored or promoted by Australia, especially in the Indo-Pacific region, are listed in '2019 Progress Report on Australia's International Cyber Engagement Strategy', available at https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_progress_report.html.

Cyber due diligence in practice

establishing both a Cooperation Group[189] and a CSIRT Network (managed by the EU Agency for Cybersecurity – ENISA)[190] which would be at the centre of information exchange concerning cyber incidents and threats. Some cooperative initiatives with similar aims have assumed a bilateral form, as in the case of the agreement between Russia and China.[191]

More generally, in its 2018 Cybersecurity Strategy, the US Department of Homeland Security highlighted its plan to be 'working with national and international partners through electronic crimes task forces to prevent, detect, and investigate various cyber crimes, including potential terrorist attacks against critical infrastructure and financial payment systems, as well as improving the security of federal facilities',[192] vowing in particular to work alongside other states' law enforcement agencies, industry representatives, and academia.[193] Of course, cooperation of this kind serves not only group interests, but also states' individual interests. Just to mention one example, after some reports of allegedly Russian-sponsored cyber operations in Montenegro, in October 2019, the US Cyber Command partnered with the local government not only to help it to increase its security, but also to bolster US cybersecurity ahead of the 2020 US presidential elections.[194]

This leads us to another popular way to cooperate internationally, i.e. sharing cyber expertise and technology with other countries, particularly developing ones. Since malicious code often travels through servers located in multiple countries, capacity-building in

189 Art. 11, NIS Directive, *supra* note 46. See also European Commission, 'NIS Cooperation Group', available at https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

190 Art. 12, NIS Directive, *supra* note 46. See also European Union Agency for Cybersecurity (ENISA), 'CSIRTs Networks', available at https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network.

191 'Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on cooperation in ensuring international information security', 30 April 2015, available at https://cyber-peace.org/wp-content/uploads/2013/05/RUS-CHN_CyberSecurityAgreement201504_InofficialTranslation.pdf.

192 US Department of Homeland Security, Cybersecurity Strategy, *supra* note 86, Objective 4.2, at 16.

193 Ibid Objective 4.3, at 17.

194 Nakasone and Sulmeyer, *supra* note 58.

Cyber due diligence in practice

other states — as a form of international cooperation — can effectively prevent and remedy harmful cyber operations, provided that the meaningful technical expertise is shared. Among many efforts of this kind are: i) Australia's regional cyber capacity-building initiative in the Indo-Pacific area, and a more specific bilateral partnership with Papua New Guinea;[195] ii) the establishment in 2018, by France, of the *École Nationale de Cybersécurité à Vocation Régionale* in Dakar (Senegal), with the aim to form cybersecurity experts in West Africa;[196] and iii) cyber security training courses organized by Japan for Vietnamese armed forces in 2017, 2019, and 2020.[197] The US has also invested over $ 70 million to help build cyber capacity in countries which 'want to act responsibly in cyberspace' and protect their networks against harmful operations by state and non-state actors.[198] In particular, the US Department of Homeland Security has expressed[199] the intention to develop 'the capacity of foreign Computer Security Incident Response Teams (CSIRTs) and law enforcement entities'.[200] In the same vein, in 2016, Japan adopted a Basic Policy to Support Cybersecurity Capacity-Building in Developing Countries, with the aim to contribute not only to other countries' cybersecurity, but also to its own, in an increasingly interconnected world.[201] Japan's Basic Policy follows three main directives: building preparedness and capacity to respond to cyber incidents, for instance by encouraging the establishment and contributing to the training of CERTs; enhancing the capacity of local law enforcement agencies to combat cyber criminality; disseminating knowledge about norms and rules of international law applicable in cyberspace.[202] Often, international

195 Australia's Cybersecurity Strategy, *supra* note 139, at 27.

196 France Diplomatie, 'L'école nationale de cybersécurité à vocation régionale de Dakar', December 2020, available at https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/nos-alliances-et-cooperations/la-cooperation-de-securite-et-de-defense/les-ecoles-nationales-a-vocation-regionale/article/l-ecole-nationale-de-cybersecurite-a-vocation-regionale-de-dakar.

197 Defense of Japan: Annual White Paper, *supra* note 107, at 389.

198 Sullivan, *supra* note 181.

199 Droit International Appliqué Aux Opérations Dans Le Cyberespace (France), *supra* note 33, at 10.

200 US Department of Homeland Security, Cybersecurity Strategy, *supra* note 86, Objective 6.3, at 24.

201 'Cybersecurity Strategy' (Japan), *supra* note 50, at 42.

202 Mihoko Matsubara, 'Japan's Cybersecurity Capacity-Building Support for ASEAN', *Palo Alto Networks Blog*, 26 July 2017, available at https://blog.

Cyber due diligence in practice

capacity-building initiatives have taken the form of financial support awarded to deserving candidates with the aim to help them improve their cybersecurity.[203]

Granted, whether those practices could be seen as specific means to comply with due diligence duties will depend on the existence of, inter alia, the requisite jurisdictional link. Nevertheless, they undoubtedly contribute to more general efforts to protect against cyber threats. On the flipside, states seeking out and benefitting from these international capacity-building efforts could be said to be acting diligently towards compliance with their own protective duties.

In addition to bilateral initiatives, cooperative capacity-building efforts have also been actively sponsored by international organizations. By way of example, the ENISA organizes every two years an EU-wide cybersecurity exercise named CyberEurope, which gives a chance to experts from member states countries to analyse complex cybersecurity incidents and get insights and suggestions on how to manage and respond to them.[204] In a telling reflection of current cyber threats, the 2020 CyberEurope scenario concerned cybersecurity incidents involving the healthcare sector.[205] Of comparable character is the cyber defence exercise known as Cyber Coalition, regularly organised by NATO for member states' defence experts.[206]

Of course, international cooperation may take other forms. It is hoped that states, especially those possessing the most advanced technology and expertise, will be open to engage in good faith in cooperative initiatives as minimum due diligence requirement or 'feasible measures' in the prevention and response to harmful cyber operations.

paloaltonetworks.com/2017/07/cso-japans-cybersecurity-capacity-building-support-asean-shifting/.

203 Recent examples include the EU 2020 CEF Telecom Cybersecurity call (https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2020-cybersecurity) and the UK's Cyber Security Capacity Building Programme 2018 to 2021 (https://www.gov.uk/government/publications/fco-cyber-security-capacity-building-programme-2018-to-2021).

204 See ENISA, 'Cyber Europe', available at https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.

205 See ENISA, 'Cyber Europe 2020', available at https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/cyber-europe-2020/.

206 More information at NATO Cooperative Cyber Defence Centre of Excellence, 'Exercises', available at https://ccdcoe.org/exercises/.

3. Conclusion: Of homework and tests

This paper has sought to show that — despite the undeniable room for further development — international law already offers wide-ranging directions on how to increase peace, security and diligent behaviour in cyberspace. In particular, it contains several due diligence obligations of general applicability, which require states to behave diligently in order to prevent, stop and respond to a range of cyber harms. These include the Corfu Channel and no-harm principles, positive obligations to protect and ensure human rights, and positive IHL duties. These rules can, and in fact are, applicable to cyberspace by effect of two alternative methods: i) either because the scope of those rules is wide enough to cover ICTs, as interpreted in light of subsequent state behaviour and attitudes with respect to those technologies — our preferred approach; or ii) because such evidence is sufficient to confirm the existence of cyber-specific versions of these rules, derived by deduction from more general ones.

As argued in Chapter 1, the UN GGE's 'voluntary, non-binding norms of responsible state behaviour in cyberspace' complement and operationalise, among others, the various international obligations of due diligence. Beyond these norms, a representative sample of state behaviour and attitudes towards ICTs constitutes evidence of diligent behaviour aimed at preventing, responding to and mitigating the effects of certain cyber harms, as required under international law. In particular, our survey of states' legal, technical, organisational, capacity-building and cooperative measures reveals that advance planning, technical expertise, and coordination among various stakeholders are instrumental in that respect. Thus, while one may be tempted to interpret 'best efforts' or 'feasible measures' as referring to the 'spur-of-the-moment' response to a particular cyber incident, our survey shows instead a strong endorsement for measures which increase preparedness and expertise ahead of future cyber incidents. After all, in common parlance, diligence is more often associated with studying consistently, doing one's homework and preparing well in advance of a test, rather than with masterful performance on the test day.

Cyber due diligence in practice

To be clear, lack of implementation of one or even more of the abovementioned measures will not necessarily result in a breach of the relevant due diligence obligation. States may mix and match different measures and tailor their own implementations policies as they wish. What ultimately matters is whether, all things considered, a state can be said to have put in their best efforts to prevent, respond to and mitigate the effects of certain cyber harms. We very much hope that our research has offered a roadmap for understanding what these best efforts may look like.

Conclusion

Conclusion

The research reflected in this Report started from a simple question: to what extent does 'due diligence' under 'international law' apply in 'cyberspace'? Yet, we found no simple answers in tackling the three key concepts informing this study – 'due diligence', 'international law' and 'cyberspace'. Rather, we came across deep controversy surrounding the nature and meaning of due diligence in international law as well as its applicability to cyberspace. To make sense of this complexity, we unpacked it into five core issues which are encapsulated in the chapters of this Report.

First and foremost, Chapter 1 addressed the applicability of international law to what is often termed 'cyberspace', a foundational question that necessarily precedes the study of 'cyber due diligence'. In particular, we assessed claims that cyberspace is a new domain or space of state activity that is prima facie carved out from the applicability of existing international law, including any rule or principle of due diligence. Likewise, we tested the assumption that cyber-specific state practice and *opinio juris* must be proved for any rule of international law to apply in cyberspace. Chapter 1 demonstrates that those claims are unfounded for a number of reasons. Specifically, rules and principles of general international law are by definition 'general', that is, the starting point is that they apply across the board to all domains, areas and types of state activity unless explicitly stated otherwise. In the same vein, international legal rules, general or specific, written or unwritten, can and should be interpreted to cover whatever type of activity that subsumes within their scope of application. Most importantly, after carrying out in-depth research into key concepts of computer science and domestic law, we found that 'cyberspace' is not a domain or space in the same way that natural or physical spaces, such as land, air, sea and outer space, are.

Instead, the term refers to a human and social phenomenon, enabled by a variety of digital technologies that allow natural and legal persons to communicate and perform their daily activities more effectively. These technologies, i.e. information and communications technologies (ICTs) span across the existing domains and have physical, logical, content and personal dimensions or components. And international

Conclusion

law does not discriminate between these and other technologies: it applies to whatever means states and individuals decide to use to perform their conduct. In this sense, it is technology-neutral. Finally, Chapter 1 delves into the relationship between rules and principles of international applicable to ICTs and their policy counterparts, including the so-called non-binding, voluntary norms of responsible state behaviour and similar recommendations. It shows that policy recommendations, even if mirroring existing international law, cannot deprive the latter of their legal force. Chapter 1 thus concludes that existing international applies by default, in its entirety, to ICTs, without prejudice to future efforts to coin new international legal rules to address one or more aspects of those technologies.

Chapter 2 then lays the groundwork for assessing *any* state duty to behave diligently in the ICT environment: it assesses what types of harm they may be required to prevent, stop or redress therein. It begins by looking at the extent to which different ICT layers, i.e. software, hardware, data and persons, can be harmed by cyber operations carried out by states or non-state entities. In doing so, this chapter engages with and demystifies the technical cybersecurity literature to paint an accurate picture of the current landscape of cyber harms to which international law applies. Chapter 2 then devises a taxonomy of cyber harms based on the features or attributes of the various ICT layers which might be harmed by different cyber operations. It finds that not only data but also software and hardware might have their confidentiality, integrity and availability compromised. By contrast, cyber operations may cause tangible or non-tangible damage to natural and legal persons, including harm to individual life, health, privacy or freedom of expression, as well as significant reputational and financial harm.

In what follows, Chapter 2 looks at the most frequent and damaging types of harmful cyber operations individually, grouping then into: Denial of Service Attacks; ransomware; spyware and other surveillance operations; Remote Access Trojans or 'backdoors'; computer viruses and worms; and several content-based cyber operations, such as disinformation and online hate speech. It then categorises harmful

Conclusion

cyber operations into different types of scenarios, depending on which states and persons may be implicated as perpetrators and victims. Chapter 2 concludes that, whether or not it is realistic to imagine a 'cyber catastrophe' at present and in the near future, harmful cyber operations are on the rise and they ultimately affect governments, corporations and, most importantly, human beings worldwide.

Chapter 3 discusses two concepts that underlie and modulate any obligation to behave diligently online and offline: sovereignty and jurisdiction. It notes that sovereignty not only grants states powers over their own territory and populations but also imposes upon them obligations to protect other states and individuals. As such, it is a functional concept, often requiring states to refrain from engaging in harmful conduct, to take preventive or remedial action and to accept lawful interference by other states in upholding rights recognised in international law. In the context of ICTs, sovereignty may follow a traditional 'territorialised' approach', applying to physical areas, infrastructure or perhaps even software and data located somewhere. But an alternative, and perhaps more realistic, way to conceptualise sovereignty over ICTs is to 'de-territorialise' it, that is, to conceive of it as applying to all kinds of ICT activities within a state's power, whether these take place inside or outside a state's territory, whilst recognising the power that non-state actors, in particular tech companies, also wield. Chapter 3 also acknowledges the debate surrounding the existence of a rule protecting sovereignty in international law, which may be breached by cyber operations causing certain physical or functional effects on the territory or usurping the inherently governmental functions of a state. The chapter then turns to the concept of jurisdiction and the extent to which it applies to ICTs. It concludes that while states still lack enforcement powers over ICTs located abroad, they can and often must exercise their prescriptive and adjudicative powers to regulate the use of such technologies within and outside their borders, provided that a jurisdictional link or basis exists in that regard.

Chapter 4 is at the core of this Report and its main contribution to the current academic and practical debates on the topic at hand. Drawing

Conclusion

on the findings of the previous chapters, it looks at the nature, status and meaning of due diligence in international law and the extent to which it applies to ICTs. The chapter begins by noting that, despite the longstanding confusion surrounding the exact meaning of that concept, in international law, 'due diligence' is better understood as a standard of conduct, even if the term is often used as a shorthand for one or more principles or rules. This standard usually refers to the behaviour required of states in preventing, halting or redressing a wide variety of harms, online and offline. Yet this standard varies across different 'protective' obligations where it is found, as well as its duty-bearers, the circumstances and fields in which they apply. Examples include 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. In keeping with the conclusions made in Chapter 1, those various protective obligations containing a standard of due diligence apply by default to ICTs, in the absence of a rule to the contrary and to the extent relevant.

Chapter 4 then focusses on four sets of protective duties which most prominently apply to cyber operations. These are: a) a state's duty not to knowingly allow its territory to be used for acts contrary to the rights of other states, known as the 'Corfu Channel' principle; b) the obligation not to cause significant transboundary harm to persons, objects and the territory of other states, known as the 'no-harm' principle; c) states' positive obligations to protect and ensure civil, political, social, economic and cultural rights under international law; and d) states' positive duties to ensure respect for international humanitarian law and to protect civilians from the effects of attacks during international or non-international armed conflict. This chapter concludes that, despite their differences and inherent flexibility, common features belie the various protective obligations identified. In particular, all arise from and are limited by a state's sovereignty, as expressed by their jurisdiction or control over territory or infrastructure. Likewise, states' protective obligations are conditioned by their capacity to act in the circumstances and by their (constructive) knowledge of the harm, even though — as a minimum

Conclusion

and in any case — they must put in place the necessary governmental apparatus enabling them to fulfil their protective duties. These rules apply concurrently and inform one another's interpretation online and offline. The 'patchwork approach' marks a paradigm shift in the understanding and conceptualisation of international law concerning diligent state behaviour in cyberspace.

Lastly, Chapter 5 puts in practice the patchwork of states' duties to exercise due diligence in their use of ICTs. It starts by confirming their applicability to those technologies by looking at a representative sample of states' diligent behaviour (or practice) and attitudes (or *opinio juris*) in the ICT environment. It then uses the same sample of laws, policies and views to propose a number of practical measures through which states can discharge their various protective duties. In particular, we suggest the adoption of legal, technical, organisational, capacity-budling and cooperation measures that together make up a comprehensive roadmap to compliance. Though not a silver bullet against all cybersecurity challenges of today and tomorrow, the existing international legal 'patchwork' of protective obligations, along with their practical implementation, provides a solid and comprehensive basis for harm prevention and accountability in the ICT environment. It is now up to states to use this valuable legal asset appropriately to maintain peace, security and stability in their use of ICTs, as well as to prevent future cyber harms – known and unknown. As conventional wisdom teaches us, prevention is always better than cure, and that is as valid online as it is offline.