Report

Virtual workshop

The protection of IT supply chains under international law

(This Workshop is organized by the Oxford Institute for Ethics, Law and Armed Conflict with the sponsorship of Microsoft. The views expressed in the background papers, presentations and discussions do not necessarily reflect the position of our sponsor.)

BLAVATNIK SCHOOL OF GOVERNMENT

OXFORD INSTITUTE FOR ETHICS, LAW AND ARMED CONFLICT

Executive Summary

On March 16th, 2021, the Oxford Institute for Ethics, Law and Armed Conflict (ELAC) held a virtual workshop, sponsored by Microsoft, on the regulation of IT Supply Chains. This workshop was part of the Oxford Process on International Law Protections in Cyberspace, a Process seeking to identify points of consensus on international legal rules and principles in their application to specific sectors, objects and activities. This workshop was the fourth one in the Oxford Process series, following on two events focused on the protection of the healthcare sector (May and July 2020) and one on the regulation of foreign digital interference in electoral processes (October 2020).

With the SolarWinds hack as its immediate catalyst, the workshop examined the range of international rules relevant to the protection of IT supply chains. The main focus of the event was on the following two overarching questions: (1) whether the characterisation of an operation as 'espionage' precludes a finding of breaches of other rules of international law, such as the rules of non-intervention and sovereignty, human rights obligations, the Corfu Channel and no-harm principles; (2) what the scope of these rules of international law is, and how they apply to the protection of IT supply chains.

Key Takeaways

There was widespread agreement among the participants on the following points:

1. *Cyber operations against IT supply chains pose unique challenges. This is due,* ***inter alia****, to their indiscriminate effects and the undermining of trust in systems that are regarded as essential for the operation of the internet.*

2. *International law applies to cyberspace, including to cyber operations against IT supply chains.*

3. *The qualification of an operation as 'espionage' does not preclude a finding that such an operation may be in violation of international law because of its means, method or effects.*

4. *It is critical to specify the scope of the relevant international legal rules and principles. Outstanding controversies around the principles of sovereignty and non-intervention, the Corfu Channel and no-harm rules, and the scope of 'jurisdiction' under international human rights law treaties, among others, continue to pose challenges to legal certainty and may have adverse consequences for the deterrent effect of these rules and principles.*

5. *Further study on the regulation of the means, methods and effects of cyber operations is required.*

Background

On March 16th, 2021, the Oxford Institute for Ethics, Law and Armed Conflict (ELAC) held a virtual workshop, sponsored by Microsoft, on the regulation of IT Supply Chains. This workshop was the fourth in the Oxford Process on International Law Protections in Cyberspace series, following on two events focusing on the protection of the healthcare sector (May and July 2020) and one on the regulation of foreign digital interference in electoral processes (October 2020).

Just as with previous Oxford Process events, the March workshop was prompted by pressing concerns over the intensification of particular types of cyber activity. On this occasion, these concerns were related to operations against IT supply chains, with the recent SolarWinds hack as a striking example and reference point for the discussions. As legal, policy and IT circles were learning more about the operation, its method, direct effects and broader implications, one important question started to dominate domestic and international conversations: was the SolarWinds operation 'mere' espionage? The workshop sought to move past the espionage label and inquire into the possibility of such operations breaching international law because of their means, methods or effects. In particular, the workshop focused on the following two overarching questions: (1) whether the characterisation of an operation as 'espionage' precludes a finding of breaches of other rules of international law, such as the rules of non-intervention and sovereignty, human rights obligations, the Corfu Channel and no-harm principles; (2) what the scope of these rules of international law is, and how they apply to the protection of IT supply chains.

Summary of Sessions

Welcome and Introduction

Prof Dapo Akande

ELAC

Prof Duncan Hollis

Temple University

Professor Dapo Akande (ELAC) and Professor Duncan Hollis (Temple University) gave the introductory remarks. Professor Akande clarified the goal of the Oxford Process, which is to effectuate a transition from the debates on the applicability of international law to cyberspace to a conversation on the specification of legal rules. Moving beyond the statement that international law applies to cyberspace, the Process seeks to examine how exactly it applies. The approach taken by this initiative, unlike the Tallinn Manual Process and the meetings of the Open-Ended Working Group on Information and Communication Technologies, is to look at specific types of activities, such as cyber operations targeting the healthcare sector, vaccine research, digital electoral interference, information operations and activities. Professor Hollis emphasised that the goal of the Oxford Process is to identify commonalities. Previous Oxford Statements have shown that more than a hundred lawyers can agree on a range of challenging legal questions.

The workshop was organised around three sessions. The first one was aimed at providing an overview of the SolarWinds and Microsoft Exchange hacks, thus introducing the participants to the landscape of threats and types of vulnerability exploitations the IT community had been observing in the past months. The second session considered whether there is or ought to be international law that applies specifically to espionage and cyber espionage. The third session, leaving the legal regulation of espionage aside, examined the possible application of other rules of international law to such cyber activities, even if the aim of the activity can be qualified as espionage.

Session I: The SolarWinds Hack: What do we Know?

Welcome and Introduction

Tom Burt

Microsoft

This session focused on the methodology of recent IT supply chains operations, and the implications of such operations for the IT sector and its users.

At the outset, **Mr Burt** noted that the cyber operations observed recently, as well as Stuxnet, NotPetya and WannaCry, all show the destructive power of cyber activities. Their effects highlight the need to work towards the clarification of rules of international law, and, if international law is found to lack adequate and sufficient protections, towards the filling of gaps through new rules and norms.

Turning to the SolarWinds hack, it was described as involving an actor, almost certainly a nation-State actor operating from Russia, using a sophisticated technique to infiltrate the network of a small software company called SolarWinds. SolarWinds have a popular application called Orion, which optimises network performance. It is most likely that the actor entered the company's environment through password spraying. The code entered into the system stood there quietly, waiting for an update to the Orion software. Once the time for the update arrived, the code dropped the malware into the build, thus becoming part of that build. This meant that it got signed with the digital certificate of SolarWinds. Thirty-three hundred customers globally and about eighteen hundred in the US applied this update from March to June 2020. Everyone who updated the software had the malware installed into their network. By not placing the malware into the source code tree, the actor escaped the use of verification systems. The malware was thus dropped in a place which made detection particularly challenging.

Once in the customers' systems, the malware again remained there quietly

Image: SolarWinds letters/ Stephen Foskett to avoid any detection systems. Then, it went to the command-and-control server, which allowed the hackers to take the information they wanted. They dropped a second-stage malware into those networks and closed the initial backdoor from the first malware to cover their tracks. At this stage, the actors could move through the users' networks, seeking credentials of network administrators. They used a variety of techniques to gain escalated privileges within those networks. These actors are still present in many of the infiltrated environments, and it is clear that they have stolen a significant amount of data.

Within the local networks entered, the hackers were moving as network administrators with full network administration capabilities. They then created identities that allowed them to access cloud services. Had the attackers stayed entirely on premises, they may have remained undiscovered. Fortunately, FireEye discovered their presence in their network: the anomalous use of cloud services allowed the detection of small digital footprints.

> “What is unique about this operation is the sophisticated use of the technique pioneered in the NotPetya attack – the compromise of a security up-date.

Mr Burt noted that, for many years, such State actors have been compromising supply chains for espionage purposes. This activity is consistent and constant. What is unique about this one is the sophisticated use of the technique pioneered in the NotPetya attack – the compromise of a security update. Back then, the attack was not just about espionage, as it also used ransomware to shut down the Ukrainian ecosystem. This, in turn, caused significant disruption to the life of Ukrainians, as well as economic destruction.

One of the remaining difficulties with the SolarWinds hack is that the community is not yet aware of the total number of victims. Some of them do not wish to report when they have been subjected to an attack.

The speaker also addressed the Microsoft Exchange Server data breach. Four vulnerabilities in the on- premises Exchange server were targeted by an actor most likely operating from China. A day before Microsoft was meant to issue a patch for the vulnerability, they saw a sudden escalation in the latter's exploitation. Learning about the patch, these actors orchestrated a campaign to compromise as many networks as they could. What was unique about this data breach was its incredible escalation.

The methods of these attacks, according to Mr Burt, pose interesting questions about the actors behind them. Ransomware operators do not typically engage in attacks that are expensive and challenging. Both the SolarWinds and Microsoft Exchange breaches were difficult, time-consuming and expensive to carry out.

In his final comments, the speaker emphasised the need to prevent such software update attacks. Update processes have to be trusted by customers. If customers cease to trust the process, companies cannot keep them secure. This is precisely why these attacks were particularly insidious.

During the discussion, one participant enquired whether the unique nature of these attacks can be summarised along three benchmarks: nature, purpose and effect. Their nature would be compromising IT supply chains to enter the system, their intent – proliferation at a very grand scale, not just to engage in targeted intervention for espionage, but to achieve much broader infiltration, and their effect being to cast doubt on the integrity of the software infrastructure. This final point was seen as raising concerns over high potential not just for immediate, but also for future harm.
According to the **Mr Burt**, it is the corruption of the update process that made these operations unique and problematic. If the actors can successfully place the malware in the build process, they get the advantage of the company's digital signature. This, of course, could have a catastrophic impact in cases where the victims are critical infrastructure providers. On intent, regardless of the aim of the attacker, which may be quite narrow, the technique used had a very wide blast radius.
The speaker reiterated that, in his view, the compromise of a vendor's update process should be inherently a violation of international law, at least for a vendor who has international customers.
The trust customers should be able to have is so fundamental to the security of the digital ecosystem that it should not be allowed for a State to compromise that update process.

> “Update processes have to be trusted by customers. If customers cease to trust the process, companies cannot keep them secure.

Session II: Beyond the Narrative of Silence: International Law

Speaker:

Naomi Hart

Essex Court Chambers

Discussants:

Asaf Lubin

Associate Professor of Law, Indiana University Maurer School of Law

Gary Corn

Professor of Law, American University Washington College of Law

Moderator:

Dapo Akande

ELAC

Dr Hart's presentation sought to clarify whether international law imposes any constraints on espionage activities. As noted by the speaker, espionage remains a ubiquitous feature of international relations. This, however, was not considered as entailing that it is a constraints-free space. Despite any perceived urgency over the protection of IT supply chains, it has to be borne in mind that the formation of rules of customary international law is an accretive process. Identification is a time-consuming forensic exercise. **Dr Hart** emphasised the need to ensure that no short-cuts are being taken just because of the urgency of the facts on the ground. The issue of the legality of activities falling under the heading of espionage can arise for governments, if they are considering countermeasures as a response (as countermeasures require prior illegality), for an international court, such as the International Court of Justice (for instance, under a compromissory clause in a treaty, such as the Vienna Convention on Diplomatic Relations), or for domestic courts. In all these contexts, the speaker opined, a black-letter positivist approach would be required.

The following points on the legal analysis of espionage activities were made by **Dr Hart**: International law has clear tools for identifying rules of customary law, and it contains a series of presumptions we can fall back on if no customary rule can be found to exist. The starting point is that states can act as they see fit in the absence of a specific prohibition. It would be really difficult to say that, as international law currently stands, states have coalesced around a view that inter-state intelligence- gathering is prohibited. One of the barriers in the identification exercise is that espionage by definition occurs in secret. It is unclear how many States carry out such operations, with what intensity and in what form. While it may be clear that certain states do engage in espionage (the UK, US and Israel, for instance), this does not provide an inclusive view of state practice. Discerning opinio juris may be even more challenging. The fact that States spy does not automatically mean that they accept they have a right to do so. Similarly, not spying does not mean that the practice is illegal. As far as we can tell from state practice and opinio juris, it is not possible to conclude that there is a rule of international law prohibiting states from engaging in espionage per se. This, however, is not the end of the analysis. Other rules of international law may constrain or positively authorise espionage in certain contexts. The difficulty that arises here is around the specification of these rules, as the scope of many of them is still heavily contested.

> “As far as we can tell from state practice and opinio juris, it is not possible to conclude that there is a rule of international law prohibiting states from engaging in espionage per se. This, however, is not the end of the analysis. Other rules of international law may constrain or positively authorise espionage in certain contexts.

The first discussant, **Professor Corn,** emphasised the importance of our starting point: are we discussing whether SolarWinds was a violation of international law, or whether supply chain methodologies more broadly are a violation of international law, or whether espionage is inconsistent with international law in whole or in part? Framing the discussion is crucial. According to **Professor Corn,** supply chain attacks are a methodology, and that methodology is not new. Supply chains are not the same in every circumstance and must be assessed separately for each operation. We now observe a shift from traditional espionage, which was much more targeted and focused, to a situation where an attacker can broaden the target set, and where the cost to gathering data is lower. The concerns here are different, as such operations implicate collateral harm. Depending on the data being taken, such operations implicate privacy in different ways. In the opinion of the discussant, the most useful question may be whether the law needs to change. **He agreed with Tom Burt that this is a moment for condemnation. But what the frame for that condemnation should be, he opined, is a matter to be considered carefully.**

The second discussant in this panel, **Dr Lubin,** advanced five key points for the consideration of the participants. First, he argued that a stringently formalistic and positivist account of the international law of intelligence should be rejected. Rather, we should adopt context, process and value-based interdisciplinary viewpoints focusing on the function intelligence plays. Only then can we appreciate espionage qua espionage. He further advanced **the view of the existence of a lex specialis of intelligence: a body of special secondary rules, institutions and enforcement mechanisms.** Second, the discussant opined that states enjoy a liberty to engage in peace-time intelligence operations under existing customary international law. This liberty was seen as a pre-requisite for the existing security system. Third, customary rules surrounding foreign intelligence operations can emerge. We have ushered in an era of intelligence legalism, and states are legally defending their activities and collaborating with partners. Fourth, internationalists have developed an obsession with sovereignty. But this may be antiquated: advocating for territorial line-drawing in the cyber age is out of touch. Fifth and finally, **the regulation of intelligence occurs at three distinct temporal stages: before, during and after an operation. For each phase, different rules and principles apply. We should consider legality and the rule of law, necessity and effectiveness, proportionality and adequate safeguards, good faith and fairness.** Rule appliers should look at SolarWinds and think about its context and these principles.

The moderator of this session, **Professor Akande,** framed the discussion by inquiring into the significance of making the claim that a certain operation constitutes espionage. Such a claim could be significant in a number of ways. First, it could be claimed that, because it is espionage, there is a different legal framework that applies. Second, it could be argued that because states engage in espionage, they have a right to do so, and no further questions of legal restraints are to be asked.

According to some participants, to fully understand the regulation of such operations, we need to disaggregate them, and consider the differences between economic and political espionage, with a potential finding that economic espionage is prohibited under international law. Other participants were not convinced that there is sufficient consensus to say that espionage for economic purposes is unlawful.

During the discussion, some participants noted the qualitative evolution of espionage operations. Previously, actors sought to hide knowledge of their activities from the public view. Now, as shown by the DNC hack, the objective is often to release the stolen records at a time calculated to have maximum political impact.

A central question in the discussion was that of prevention. In the absence of a consensus over norms of restraint, and yet in the presence of so

Image: Pixabay

many clashes of interests over norms of restraint, why would adversaries stop their pernicious activities and how can they be convinced to stop? It was noted that norm-transgressors have every interest in preventing the clarification of rules, and the development of new rules to govern this space. Relatedly, one interpretation given to the Microsoft Exchange hack was that the actors sought to show that this is an activity they can freely engage in. Participants agreed that rules need to be clear if we expect states to follow a certain type of conduct.

> Rules need to be clear if we expect States to follow a certain type of conduct.

There was widespread agreement that the label espionage does not preclude a finding of a violation, where the means, methods and effects of espionage operations fall foul of international legal rules. According to some, that regulation of means, methods and effects exists only at the outer boundaries of what our concerns regarding IT supply chains operations are. For the SolarWinds hack, some participants considered that we can discern a clear vulnerability vector, which may allow a finding of illegality on the means, methods or effect plane. An analogy with armed conflict was drawn: while parties to a conflict may have a right to target certain objectives, there are limitations on the ways that the targeting can occur. In the context of IT supply chain operations, some considered that tainting the entire supply chain may not be an accepted methodology. For some participants, the discussion showed that international law, as it currently stands, is insufficient to meet our protection needs and has to evolve. To achieve incremental change, this change needs to be seen as building on processes that are familiar to the audience.

Session III: International Law and the Protection of IT Supply Chains

Speaker:

Russell Buchan

University of Sheffield

Discussants:

Kristen Eichensehr

University of Virginia

Ciaran Martin

University of Oxford

Moderator:

Duncan Hollis

Temple University

Despite the lack of specific regulation of espionage under international law, Dr Buchan's argument in his presentation was that international law does have a set of rules and principles that can constrain operations classified as espionage. These rules come from a variety of fields, including international human rights law, international economic law and diplomatic law. It is critical, he argued, to identify the place or location from which espionage occurs (from a national territory or outer space, for instance); who the responsible actor is (state or non-state actor); and the type of information collected (critical information or trade secrets of a private company).

According to the speaker, territorial sovereignty is a rule that is of particular relevance in this space. It is a rule that permits states to exercise governmental functions free from interference. Just as non- consensual trespass in state territory in the physical world is seen as a clear violation of the principle, operations that 'trespass' into sovereign cyber territory should be seen as breaching the law. The principle should be divorced from the idea of harm and damage. For instance, focusing on operations requiring significant remedial action would bring additional challenges, as this requirement would subjectify the application of the principle. By divorcing the rule from these requirements, we would more closely align with its application in the physical world, and also give it a more meaningful scope in cyberspace.

The first discussant, **Professor Eichensehr**, in responding to the speaker, noted that the state of play is quite mixed with respect to the rule on sovereignty: quite a few states do not recognise territorial sovereignty as a standalone rule. Even states recognising it do not necessarily agree on its scope. There is substantial variation of state practice. The discussant opined that **a crucial question concerns the risk levels states are ready to accept.** Should we be focusing on preventing disruption or escalation? Some states seem to be drawing a line around disruption, but there is still very little clarity over the accepted thresholds. And finally, Professor Eichensehr noted that states have not failed to regulate espionage; rather, they have done so in their domestic systems through criminalisation and tools for enforcement. Domestic regulation may have an impact on individual deterrence, and it could also incentivise disclosures and cooperation with other states.

> Many participants considered human rights law to be a fruitful avenue for thinking about the impact of such operations.

Professor Martin, the second discussant in this session, **emphasised the need to keep these legal assessments close to the operational reality of how states see such operations.** He agreed with the scepticism around territorial sovereignty as a rule expressed by the first discussant. Thinking about the future steps of the Oxford Process, he suggested tying the legal discussion to geopolitical imperatives and an acknowledgment that espionage can sometimes have a useful function.

In the open discussion, participants raised a number of areas of law that have relevance for the regulation of operations impacting IT supply chains. **Many participants considered human rights law to be a fruitful avenue for thinking about the impact of such operations, as individuals can find themselves their intended or unintended targets.** Particular rights discussed were privacy, health, life, expression and property. It was noted that the main challenge facing such claims under human rights law is the controversy over the content of extraterritorial jurisdiction.
The importance of discussing the responsibility of businesses to respect rights was also highlighted by some participants.

Related to the transition from a perpetrator's perspective to a victim's perspective, the moderator, **Professor Hollis, noted the significance of remaining mindful of the externalities and spill-over that operations such as SolarWinds cause. These externalities and spill-over effects are connected to a broader discussion on the risks and threats inherent in IT supply chain attacks using the methods recently observed.** One participant noted that these risks and threats were highlighted in the 2021 OEWG Report.
On the point of lex ferenda, some participants raised the possibility of fleshing out rules that protect the public core of the internet.

Concluding remarks

At the end of the session, **Professor Akande** identified some of the commonalities discerned during the discussion.

First, it seems that **the most serious concern** is over **operations that damage trust in systems that are regarded as essential for the operation of the internet.** The question, then, is whether there are any legal rules that constrain cyber operations against such systems. A potential obstacle to articulating these rules is that the operations are often conducted for the purpose of espionage.

Second, the purpose of espionage raises a new host of questions: is there special regulation of espionage under international law? Is there a right to engage in espionage? There seemed to be broad consensus that **simply labelling something 'espionage' does not mean there is a lack of legal regulation, ie the label does not place the operation beyond international regulation.**

Third, there is **a need to look deeper at the means, methods and effects of operations.** The relevant **principles and rules** – sovereignty, human rights and others – are **in need of further specification.**

List of Participants

1. **Christiane Ahlborn,** Legal Officer, UN Office of Legal Affairs
2. **Dapo Akande,** Professor of Public International Law, Co-Director, Oxford Institute for Ethics, Law & Armed Conflict (ELAC), University of Oxford
3. **Leonie Arendt,** Policy Consultant, UN Foundation
4. **Karine Bannelier-Christakis,** Associate professor of International Law, Université Grenoble Alpes
5. **Nayia Barmpaliou,** Non-Resident Expert, Cybersecurity, European Union Institute for Security Studies
6. **Russell Buchan,** Senior Lecturer in International Law, University of Sheffield
7. **Tom Burt,** Corporate Vice President, Customer Security & Trust, Microsoft
8. **Scott Charney,** Vice President, Security Policy, Microsoft
9. **Kaja Ciglic,** Senior Director, Digital Diplomacy, Microsoft
10. **Antonio Coco,** Lecturer in Public International Law, University of Essex and Visiting Fellow at ELAC, University of Oxford
11. **Gary Corn,** Professor of Law and Director of Technology, Law & Security Program, American University Washington College of Law
12. **Enrico Cossidente,** Italian Army staff officer and military legal advisor
13. **Jennifer Daskal,** Deputy General Counsel, US Department of Homeland Security
14. **Francois Delerue,** Research Fellow in Cyberdefense and International Law, Institute of Strategic Research of the Military Academy, France
15. **Miguel de Serpa Soares,** Under-Secretary-General for Legal Affairs and United Nations Legal Counsel
16. **Talita Dias**, Research Fellow, Jesus College & ELAC, University of Oxford
17. **Kristen Eichensehr,** Martha Lubin Karsh and Bruce A. Karsh Bicentennial Professor of Law, University of Virginia
18. **David Fidler**, Adjunct Senior Fellow for Cybersecurity & Global Health, Council on Foreign Relations
19. **Naomi Hart,** Barrister, Essex Court Chambers
20. **Duncan Hollis,** Laura H. Carnell Professor of Law, Temple University School of Law
21. **Zhixiong Huang**, Professor of International Law & Vice Dean for International relations, Executive Director, Wuhan University Institute for Cyber Governance, Wuhan University
22. **Graham Ingram,** Chief Information Security Officer, University of Oxford
23. **Katie Johnston,** DPhil candidate in International Law, University of Oxford
24. **Kate Jones,** University of Oxford
25. **Andraz Andy Kastelic,** Lead cyber stability researcher, Security and Technology Programme, UNIDIR
26. **David Kaye,** Clinical Professor of Law, University of California, Irvine
27. **Lucas Kello,** Associate Professor of International

List of Participants

Relations, University of Oxford

28. **Harold Hongju Koh**, Senior Adviser and former Legal Adviser (2009-13), Office of the Legal Adviser, US Department of State
29. **Jeffrey Kovar,** Assistant Legal Adviser for Political-Military Affairs, US Department of State
30. **Leonhard Kreuzer,** Research Fellow, Max Planck Institute for Comparative Public Law and International Law
31. **Joanna Kulesza,** Professor of Law, University of Lodz
32. **Masahiro Kurosaki,** Associate Professor of International Law and Director of the Study of Law, Security and Military Operations, National Defense Academy of Japan
33. **Grace L,** GCHQ
34. **Henning Lahmann,** Senior Researcher, Digital Society Institute, ESMT Berlin
35. **Marja Lehto**, Ambassador and Senior Legal Expert, Minister of Foreign Affairs, Finland
36. **Asaf Lubin,** Associate Professor of Law, Indiana University Maurer School of Law
37. **Kubo Mačak**, Legal Adviser, International Committee of the Red Cross, Associate Professor, University of Exeter
38. **Nemanja Malisevic,** Director, Digital Diplomacy International Lead, Defending Democracy Program, Microsoft
39. **Ciaran Martin,** Professor of Practice, Blavatnik School of Government, University of Oxford
40. **Tomohiro Mikanagi,** Deputy Director-General of the International Legal Affairs Bureau, Ministry of Foreign Affairs of Japan
41. **Tomáš Minarik**, Head of International Organisations and Law Unit, National Cyber and Information Security Agency of the Czech Republic
42. **Harriet Moynihan,** Senior Research Fellow, International Law Programme, Chatham House
43. **Jan Neutze**, Senior Director, Digital Diplomacy, Microsoft
44. **Kazuho Norikura,** Ministry of Foreign Affairs, Japan
45. **Jim O'Brien,** Vice Chair, Albright Stonebridge Group
46. **Giacomo Persi Paoli,** Programme Lead for Security and Technology Programme, UNIDIR
47. **Patryk Pawlak,** Executive Officer, European Union Institute for Security Studies
48. **Przemysław Roguski,** Lecturer in Law, Jagiellonian University in Kraków
49. **Vera Rusinova**, Professor of International Law, Higher School of Economics in Moscow
50. **Michael Schmitt**, Professor of International Law, University of Reading; Francis Lieber Distinguished Scholar at the Lieber Institute of the United States Military Academy (West Point)
51. **Corinna Seiberth,** Lawyer, Federal Department of Foreign Affairs FDFA, Directorate of International Law, International Law Division, Switzerland
52. **Nicola Smith,** Legal Counsellor and Head of the National Security Team, FCDO

List of Participants

53. **Marcus Song,** Senior State Counsel, International Affairs Division, Attorney-General's Chambers, Singapore
54. **Hansjoerg Strohmeyer,** Chief of Policy Development and Studies Branch, United Nations Office for the Coordination of Humanitarian Affairs
55. **Nikhil Sud,** Regulatory Affairs Specialist, Albright Stonebridge Group
56. **Masaru Suzuki,** First Secretary, Embassy of Japan in the United Kingdom
57. **John Swords,** Legal Adviser and Director of the Office of Legal Affairs at NATO Headquarters
58. **Wieteke Theeuwen,** Legal Officer, International Law Division, Ministry of Foreign Affairs of The Netherlands
59. **Tsvetelina van Benthem,** Research Officer, ELAC
60. **Liis Vihul,** Chief Executive Officer, Cyber Law International
61. **Marguerite Walter,** Attorney-Adviser, Human Rights and Refugees, Office of the Legal Adviser, US Department of State
62. **Alexander Wentker,** DPhil candidate in International Law, University of Oxford
63. **Stephen Wheatley,** Professor of International Law, University of Lancaster
64. **Robert Young,** Legal Counsel, Global Affairs Canada

OXFORD INSTITUTE FOR ETHICS, LAW AND ARMED CONFLICT

BLAVATNIK SCHOOL OF GOVERNMENT

OXFORD INSTITUTE FOR
ETHICS, LAW AND
ARMED CONFLICT