OXFORD INSTITUTE FOR ETHICS, LAW AND ARMED CONFLICT

Microsoft

BLAVATNIK SCHOOL OF GOVERNMENT

UNIVERSITY OF OXFORD

JAPANGOV
THE GOVERNMENT OF JAPAN

REPORT

Virtual Workshop

APPLYING INTERNATIONAL LAW IN CYBERSPACE: PROTECTIONS AND PREVENTION

18-19 May 2020

Oxford Institute for Ethics, Law and Armed Conflict (ELAC)

18 – 19 May 2020

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

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

Session #1: International Law Protections against Malicious Cyber Operations Targeting the Healthcare Sector

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

To understand the importance of this topic, it is important to realise that the current crisis brings to light both our shared humanity and our shared vulnerability. This vulnerability created by the virus is further exacerbated by our dependence on networks. For instance, the functioning of a hospital can be paralysed by a ransomware attack. Given the risk of loss of life inherent in such attacks, even cyber criminals have recently vowed not to target healthcare facilities.

It was emphasised that these cyber operations do not occur in a legal void: international law applies in cyberspace. One of the relevant regimes that were examined was international humanitarian law (IHL), which

'Cyber operations do not occur in a legal void: international law applies in cyberspace'

provides robust legal protection in times of armed conflict. Importantly, IHL applies to all means and methods of warfare and covers cyber operations of belligerent parties. Despite some fears that the applicability of IHL to cyberspace could militarise the domain, such a trend has not been observed, according to the presenter, and IHL places important restrictions on the actions of belligerents. In particular, IHL requires that medical units and personnel must be respected and protected at all times. Respect translates into an obligation not to disrupt the facilities and to take all feasible precautions against incidental harm. Protection requires steps taken to avoid or minimise harm from others. As noted by the presenter, it is hard to conceive of a cyber operation aimed against medical facilities in armed conflict that would somehow be lawful under IHL. Outside of armed conflict, healthcare facilities are protected by other rules of international law, including international human rights law (IHRL).

During the presentation, a new norm of responsible state behaviour proposed by the International Committee of the Red Cross was discussed: 'States should not conduct or knowingly support [cyber] activity that would harm medical services or medical facilities, and should take measures to protect medical services from harm.' This norm was seen as reaffirming existing rules of international law. One strand of criticism against the adoption of this norm takes the view that presenting it as 'new' would suggest the lack of an existing legal framework or its insufficiency. Another strand of criticism takes issue with the focus on the medical context, as this may be seen as suggesting that other critical infrastructure is not similarly protected. The presenter took the view that the addition of a layer of legal protection cannot detract from what the law already provides, that is, that existing protections remain intact and the new norm only serves to fortify the legal protection of medical infrastructure and to emphasise its vulnerability. As was highlighted by some participants in the open discussion, another potential difficulty with the advancement of a new norm is that there are significant risks of a stalemate in inter-governmental forums if such a new norm is placed on the table.

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

Additionally, the discussant saw the thresholds of the use of force and armed attack as another area of uncertainty. While a lot of attention has been given to the *degree* of harm to infrastructure, the same cannot be said

of the *types* of injury that may rise to the level of an attack, and in particular, injuries that relate to mental health conditions, such as post-traumatic stress disorder.

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

Harriet Moynihan was the discussant on May 19th, and she addressed in more detail the element of coercion in the prohibition of intervention, the potential thresholds for a violation of the non- intervention rule, and the question whether sovereignty exists as a rule or a principle. On coercion, she noted that the element need not be confined to an interpretation that emphasises the dictation of a course of conduct; in fact, the element may be seen as centring on a wrongful deprivation of choice, an act that effectively deprives a State of control over matters of an essentially sovereign nature. On thresholds, she stressed the need for clear benchmarks in assessing a potential *de minimis* line. These benchmarks are necessary to draw boundaries, in particular on the low end of interference. This would allow us to qualify a range of operations, such as those bearing resemblance to espionage, for instance, operations gathering information on the number of patients in a hospital. On sovereignty, the discussant considered whether it is possible to speak of a legal obligation if there is such difficulty in determining its substantive contours.

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

On the prohibition of intervention, some participants questioned whether the element of coercion necessarily implies an action taken to force another State into pursuing, or abstaining from pursuing, a particular line of conduct. It was considered whether coercion could also be interpreted to cover cases where an actor disrupts or inhibits the activities of a State without necessarily advancing any demands. Such action would encroach upon areas in which the State can decide freely, in choices that must remain free ones. An example given was when the target State, as a result of a cyber operation, becomes unable to control its healthcare system. According to other participants, this interpretation of the element of coercion hides the risk of overreach, as it would extend to the exercise of any jurisdictional power within the State's *domaine réservé*. Others saw difficulties in drawing the line between influence and coercion, and in finding practice supporting the existence of coercion beyond cases involving the use of force.

A related topic that was addressed during the discussion was the existence of a rule of sovereignty separate from the prohibition of intervention. To some, the alternative interpretations of the element of coercion under the non-intervention rule are merely workarounds attempting to circumvent the acknowledgement that a self-standing rule of sovereignty exists. It was noted that States from continental Europe increasingly accept the existence of such a self-standing rule of sovereignty which protects the exercise of governmental powers without a State's permission. Another angle of the discussion on sovereignty centred on the types of intrusion that the rule could cover. In particular, the confidentiality, integrity and availability of systems were seen as pertinent benchmarks to look at, although the precise nature and extent of interference required to reach the level of prohibited conduct remain unclear.

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

According to some participants, more attention should be paid to certain well-established rules that could cover a broad range of low-intensity operations, such as the constant care obligation under IHL.

Some commentators considered that a focus on IHL and the framework of the resort to force may give rise to heated debates, and, ultimately, an impasse in inter-governmental dialogues that would detract from the careful examination of important peacetime rules, such as the range of due diligence duties.

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

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

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

'For cyber attacks against medical facilities, we observe a *unique lack of justification*.'

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

Session #2: States' Obligations of Due Diligence in Cyberspace

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

The first presentation was based on a paper prepared by **Antonio Coco** and **Talita de Souza Dias** entitled 'More than Meets the Eye: A Patchwork of Cyber Due Diligence Duties in International Law'. Some strands of their research on due diligence in the context of Covid-19 can be found here, here and here.

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

According to the authors of the paper, the debate on whether a standalone rule of cyber due diligence exists misses the point: several duties to behave

'Several duties to behave diligently to prevent, halt and/or redress cyber harms already undoubtedly exist in international law'

diligently to prevent, halt and/or redress cyber harms already undoubtedly exist in international law. It was emphasised that international law in its entirety applies to cyberspace by default and that State practice and *opinio juris* support this reading. Clarity about the various due diligence obligations of States can help maintain a more secure cyberspace.

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

Heike Krieger was the discussant of the first presentation on May 19th. She suggested focussing on the no-harm principle, which is not restricted to environmental law and may give the most viable option forward. Its viability can be traced back to its broad sphere of application – to lawful and unlawful behaviour, for acts by States and non-State actors. She agreed that due diligence is a standard, not a rule: the applicable rule would be the no-harm principle, not due diligence as such. The discussant placed an emphasis on procedural obligations, such as the duties to notify, inform, consult, publicly explain, as they are concrete and serve to create trust.

In the **open discussion** moderated by **Dapo Akande**, some commentators emphasised the need to attach the concept of due diligence to specific primary rules. This is because one cannot say that States are obliged to act diligently *in general*, they have specific obligations in specific contexts. The term 'due diligence' says nothing on what kind and degree of diligence is

due. A fear expressed was that a general discussion of due diligence may dilute our understanding of State obligations: in many cases, States have obligations that require more than diligence, one example being human rights law with its tests of legitimate aims and proportionality.

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

It was noted by a number of participants that the presentations only addressed the 'after' question, i.e. once a State is aware of a malicious cyber operation. A difficult question is raised in the 'before' period – is there an obligation to be aware of specific risks? Taking this to the context of the current pandemic, perhaps a State with few resources in its healthcare sector will have no capacity to monitor what is happening in its cyber environment. The question then is whether it *should have been aware*, and this is a question that pertains to the factual triggers of such obligations. Deliberate ignorance would not be acceptable.

Still, on the level of factual triggers, some participants expressed concern over the impact that these obligations may have on the right to privacy. This question was seen as linking back to the discussion of primary obligations and the knowledge standard incorporated in such primary rules. According to one of the presenters, knowledge could be examined in two ways: first, as a procedural obligation to acquire the minimum capacity or infrastructure enabling the State to obtain the necessary information, and second, a due diligence obligation triggered when there is a foreseeable risk of a forthcoming cyberattack. The duty to monitor would also depend on capacity. A balance is to be found when considering potentially conflicting duties of the State, and this balance can be found, for example, in concrete tests, such as those existing under IHRL.

The relationship between due diligence, sovereignty and extraterritorial jurisdiction was also considered. One of the presenters affirmed that all States which have sovereignty have due diligence obligations rooted in the very fact of statehood, as they have a governmental apparatus.

Apart from the specific issues arising out of the need to clarify primary rules containing due diligence standards, the participants discussed the value of engaging in this exercise. Some participants saw the utility of due diligence in that it offers an alternative to the 'attribution' route. Due diligence comes into play when there is a risk to be managed (technical,

Due diligence may offer an alternative to the 'attribution' route

environmental, coming from another actor) and States are obliged to eliminate or contain that risk.

And while the participants saw the utility of analysing due diligence obligations, some noted the terminological confusion that these standards have provoked. One commentator opined that 'due diligence' in cyberspace has been mainly associated with the Corfu Channel principle. An approach suggested by one participant was to determine whether everyone agrees that the Corfu principle exists under customary law; if so, then the policy debate should be seen as an attempt by some to carve out a rule *excluding* cyberspace from the principle, rather than as a discussion on whether the rule exists.

During the discussion on procedural obligations arising from the due diligence standard some participants cautioned against an emphasis on notification requirements without carefully investigating their implications. There could be a concern that a duty to notify may in effect require States to reveal their capacities to other States.

Finally, the main value of these discussions was seen in the exercise of unpacking what 'reasonableness' in the context of various due diligence standards means, and how States are required to act in specific circumstances. For instance, in the context of extraterritorial jurisdiction under IHRL, reasonableness was seen as an important constraining element: without it, the mere ability of a State to influence something somewhere may be seen as implying that the obligation has been triggered. Additionally, reasonableness plays a role at the stage of determining what measures a State can reasonably be expected to take.

***

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

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

In line with the call for a clarification of legal standards issued in the closing remarks, the Oxford Statement was referred to UN member States. The Oxford Statement was

mentioned as a good example of how international law applies in cyberspace by the representative of the Dominican Republic, Ambassador, Special Envoy to the Security Council, H.E. Mr. José Singer Weisinger, one of the co-hosts of the UN Security Council Arria-Formula Meeting on Cyber Stability and Responsible State Behaviour in Cyberspace that took place on Friday, 22 May 2020.

OXFORD INSTITUTE FOR ETHICS, LAW AND ARMED CONFLICT

VIRTUAL WORKSHOP

APPLYING INTERNATIONAL LAW IN CYBERSPACE: PROTECTIONS AND PREVENTION

18 May 2020

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

PROGRAMME AND LIST OF PARTICIPANTS

PROGRAMME

9 AM (Oxford): Welcome and introductions

9.15 AM: International Law Protections against Malicious Cyber Operations Targeting the Healthcare Sector

- Presentation by K. Maćak, L. Gisel, T. Rodenhäuser, ICRC Legal Division
- Discussant: R. Liivoja, University of Queensland
- Open Discussion

10.35 AM: BREAK

10.40 AM: States' Obligations of Due Diligence in Cyberspace

- Presentation by T. de Souza Dias, Oxford Institute for Ethics, Law and Armed Conflict
- Presentation by T. Mikanagi, Ministry of Foreign Affairs of Japan
- Open Discussion

12 PM: Concluding remarks – Harold Koh

LIST OF PARTICIPANTS

1) Dapo AKANDE, Professor of Public International Law, Co-Director, Oxford Institute for Ethics, Law & Armed Conflict, University of Oxford
2) Russell BUCHAN, Senior Lecturer in International Law, University of Sheffield
3) Kaja CIGLIC, Senior Director, Digital Diplomacy, Microsoft
4) Antonio COCO, Lecturer in Public International Law, University of Essex and Visiting Fellow at ELAC, University of Oxford
5) Rebecca CROOTOF, Assistant Professor of Law, University of Richmond
6) Talita DE SOUZA DIAS, Postdoctoral Research Fellow, ELAC, University of Oxford
7) Laurent GISEL, Senior Legal Adviser, International Committee of the Red Cross
8) Duncan HOLLIS, Professor of Law, Temple University
9) Zhixiong HUANG, Professor of International Law & Vice Dean for International relations,
   Executive Director, Wuhan University Institute for Cyber Governance, Wuhan University
10) Tania JANCARKOVA, NATO Cooperative Cyber Defence Centre of Excellence
11) Kate JONES, Director of the Oxford Diplomatic Studies Programme, University of Oxford
12) Harold Hongju KOH, Sterling Professor of International Law, Yale Law School
13) Masahiro KUROSAKI, Associate Professor of International Law and Director of the Study of Law, Security and Military Operations, National Defense Academy of Japan
14) Rain LIIVOJA, Associate Professor of Law, University of Queensland
15) Kubo MAČAK, Associate Professor of International Law, University of Exeter and Legal Adviser, International Committee of the Red Cross

16) Nemanja MALISEVIC, Director, Digital Diplomacy International Lead, Defending Democracy Program, Microsoft
17) Eviatar MATANIA, Professor at the School of Political Science, Government and International Affairs, Tel Aviv University
18) Suzuki MASARU, First Secretary, Embassy of Japan in the United Kingdom
19) Tomohiro MIKANAGI, Deputy Director-General of the International Legal Affairs Bureau, Ministry of Foreign Affairs of Japan
20) Tomáš MINÁRIK, Head of International Organisations and Law Unit, National Cyber and Information Security Agency of the Czech Republic
21) Jim O'BRIEN, Vice Chair, Albright Stonebridge Group
22) George PAPADEMETRIOU, Analyst, Albright Stonebridge Group
23) Patryk PAWLAK, Executive Officer, European Union Institute for Security Studies – Brussels
24) Anne PETERS, Managing Director, Max Planck Institute for Comparative Public Law
25) Tilman RODENHAUSER, Legal Adviser, International Committee of the Red Cross
26) Przemysław ROGUSKI, Lecturer in Law, Jagiellonian University in Kraków
27) Antonios TZANAKOPOULOS, Associate Professor of Public International Law, University of Oxford
28) Tsvetelina VAN BENTHEM, DPhil Candidate in Public International Law, University of Oxford
29) Yuki YASUDA, Ministry of Foreign Affairs of Japan

OXFORD INSTITUTE FOR ETHICS, LAW AND ARMED CONFLICT

Microsoft

BLAVATNIK SCHOOL OF GOVERNMENT

UNIVERSITY OF OXFORD

JAPANGOV
THE GOVERNMENT OF JAPAN

VIRTUAL WORKSHOP
APPLYING INTERNATIONAL LAW IN CYBERSPACE: PROTECTIONS AND PREVENTION
19 May 2020

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

PROGRAMME AND LIST OF PARTICIPANTS

PROGRAMME

4.00 PM (Oxford): Welcome and introductions

4.15 AM: International Law Protections against Malicious Cyber Operations Targeting the Healthcare Sector

- Presentation by K. Maćak, L. Gisel, T. Rodenhäuser, ICRC Legal Division
- Discussant: H. Moynihan, Chatham House
- Open Discussion

5.35 PM: BREAK

5.40 PM: States' Obligations of Due Diligence in Cyberspace

- Presentation by A. Coco, Oxford Institute for Ethics, Law and Armed Conflict
- Discussant: H. Krieger, Freie Universität Berlin
- Open Discussion

7.00 PM: Concluding remarks – Harold Koh

LIST OF PARTICIPANTS

1) Dapo AKANDE, Professor of Public International Law, Co-Director, Oxford Institute for Ethics, Law & Armed Conflict, University of Oxford
2) Meredith BERGER, Senior Manager, Defending Democracy Program, Microsoft
3) Marjolein BUSSTRA, Legal Counsel, Netherlands Ministry of Foreign Affairs
4) Scott CHARNEY, Vice President, Security Policy, Microsoft
5) Sarah CLEVELAND, Louis Henkin Professor of Human and Constitutional Rights and Co- Director of the Human Rights Institute, Columbia University Law School
6) Antonio COCO, Lecturer in Public International Law, University of Essex and Visiting Fellow, ELAC, University of Oxford
7) Federica D'ALESSANDRA, founding Executive Director of the Oxford Programme on International Peace and Security, ELAC, Blavatnik School of Government, University of Oxford
8) Francois DELERUE, Research Fellow in Cyberdefense and International Law, Institute of Strategic Research of the Military Academy, France
9) Talita DE SOUZA DIAS, Postdoctoral Research Fellow, ELAC, University of Oxford
10) Kristen EICHENSEHR, Assistant Professor of Law, UCLA Law School
11) Laurent GISEL, Senior Legal Adviser, International Committee of the Red Cross
12) Claudio GROSSMAN, Professor of Law, Dean Emeritus, American University Washington College of Law
13) Duncan HOLLIS, Professor of Law, Temple University
14) Miles JACKSON, Associate Professor of Law, University of Oxford
15) Eric JENSEN, Professor of Law, Brigham Young University
16) Heike KRIEGER, Professor of International and Public Law, Freie Universität Berlin
17) Harold Hongju KOH, Sterling Professor of International Law, Yale Law School
18) Henning LAHMANN, Senior Researcher, Digital Society Institute, ESMT Berlin

19) Kubo MAČAK, Associate Professor of International Law, University of Exeter and Legal Adviser, International Committee of the Red Cross
20) Harriet MOYNIHAN, Senior Research Fellow, International Law Programme, Chatham House
21) Jan NEUTZE, Senior Director, Digital Diplomacy, Microsoft
22) Georg NOLTE, Professor of International Law, Humboldt University Berlin
23) Jim O'BRIEN, Vice Chair, Albright Stonebridge Group
24) Daniela RAKHLINA-POWSNER, JD Candidate, Temple University
25) Tilman RODENHÄUSER, Legal Adviser, International Committee of the Red Cross
26) Barrie SANDER, Postdoctoral Fellow, FGV Direito Rio
27) Michael SCHMITT, Professor of Public International Law, University of Reading
28) Tsvetelina VAN BENTHEM, DPhil Candidate in Public International Law, University of Oxford
29) Liss VIHUL, Chief Executive Officer, Cyber Law International
30) Douglas WILSON, Director of Legal Affairs, GCHQ
31) Elizabeth WILMSHURST, Distinguished Fellow, International Law Programme, Chatham House
32) Alexander WIRTH, Cybersecurity Strategist, Defending Democracy Program, Microsoft
33) Robert YOUNG, Legal Counsel, Global Affairs Canada