

Report

Virtual workshop

The Oxford Process on International Law Protections in Cyberspace: Safeguarding the Covid-19 vaccine research

(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

THE
OXFORD
PROCESS

31 July 2020

Executive Summary

On July 31st, 2020, the Oxford Institute for Ethics, Law and Armed Conflict (ELAC) held a virtual workshop, sponsored by Microsoft, on the international legal rules that protect vaccine research. This workshop was part of the Oxford Process on International Law Protections in Cyberspace, an initiative seeking to identify points of consensus on international legal rules and principles in their application to specific sectors, objects and activities. This workshop was the second one in the Oxford Process series, following on from a workshop on the protection of the healthcare sector (May 2020).

Cyber operations targeting institutions engaged in vaccine research started almost as soon as the research itself. These operations exposed vulnerabilities in the networks of research institutions and served as a stark reminder of the importance of protecting the development of a vaccine. During the workshop, the protection of vaccine research was reviewed through an array of disciplines: from cybersecurity through policy to law. This combination of perspectives painted a detailed picture of the threat landscape and the types of harm that cyber operations may cause.

Key Takeaways

The following points emerged from the discussion:

- 1.** *Cyber operations against vaccine research present complex challenges. Even operations that do not seek the disruption or destruction of systems and/or data can damage the integrity of vaccine trials, thus slowing down the approval, production and distribution of the vaccine.*
- 2.** *International law is an essential component of the toolkit that states and other actors can use to deter harmful behaviour. Its applicability to information and communications technologies (ICTs) was a point of agreement among participants.*
- 3.** *For international law to fulfil its purpose, how it applies to cyber operations against vaccine research should be clarified. This would involve a process of specification of the relevant international legal rules.*
- 4.** *International law already contains a range of relevant and applicable binding legal rules that constrain the behaviour of states and other actors and require the taking of positive steps to protect vaccine research.*
- 5.** *The contours of many rules of international law remain pixelated. More work is needed on the meaning of 'harm', a requirement of intentionality in particular rules, and the types of measures through which obligations with a due diligence standard can be discharged, among others.*

Background

As the fight against Covid-19 continues in hospitals, public and private health institutions, laboratories and research facilities around the world, so do cyber operations targeting or disrupting these efforts. In this context, the Oxford Institute for Ethics, Law and Armed Conflict (ELAC), co-sponsored by the Government of Japan and Microsoft, hosted a virtual workshop in May 2020 to discuss states' obligations to refrain from cyber operations against the healthcare sector and to protect it from a range of online harms. Those discussions resulted in the Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Healthcare Sector, signed by over 130 international lawyers and cited as a model of how international law applies in cyberspace during the 2020 UN Security Council Arria-Formula meeting on the issue.

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

Summary of Sessions

Welcome and Introduction



Prof Dapo Akande

ELAC

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

The second workshop was driven by a need for granularity in international legal protections, made particularly acute by the increase in cyber operations against institutions engaged in vaccine research. Just as with the previous session of the Oxford Process, the aim was to identify

areas of consensus on existing protections under international law. These areas of consensus would then become the basis of a second Oxford Statement. Amid a raging pandemic, clarifying how international law applies to vaccine research – the activity that can free us from the grasp of the disease – was critically important. Specifically, it can serve as a pathway to bolstering the protective measures taken by states, a deterrent to potentially harmful conduct, and a vehicle for articulating claims of violations of the law.

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

Session I: Presentations



Presentation 1

Graham Ingram

Chief Information Security
Officer, Oxford

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

Mr Ingram introduced the workshop participants to the objective of Oxford University's cyber defence team: preventing a cyber event from materialising. To attain this objective, both preventative and reactive control measures play a key role, as it is their combination that can ensure the mitigation of the likelihood of damage to University networks. Cyber delivery and maintenance involve a combination of people, processes and technologies across the University, private sector partners and the UK government.

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

Universities do not have a reputation for high levels of cyber security, and this can be explained by the methods through which academic institutions operate. Research is usually conducted in partnership with others and requires a high degree of openness. Cybersecurity involves a combination of confidentiality, integrity, and availability of ICT systems. Confidentiality, however, cannot be



Even the best reactive controls cannot eliminate all risk. A legal framework of preventative control can be beneficial in combating harmful behaviour online.

maintained at a high level due to the openness of university research. Integrity and availability become critically important, especially in the context of clinical trials. For a range of reasons, universities do not benefit from the cyber protection that governments have, and the most determined actors will find their way in.

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



Presentation 2

Doug W

Director of Legal Affairs and
International Relations, GCHQ

(Speaking in a personal capacity)

Photo: GCHQ/Crown Copyright

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

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

influence of private actors in the setting of international standards in the field of privacy protection.

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

Experience had played an important role in shaping the UK approach to such incidents.

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

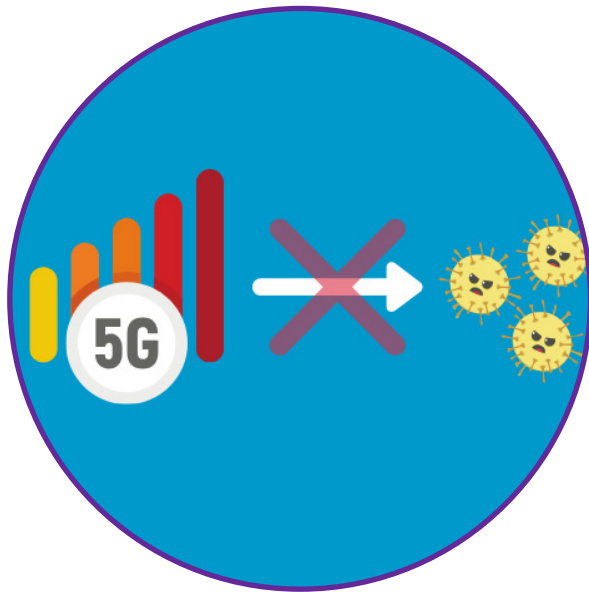
Moving to domestic law, the 1990 Computer Misuse Act heavily relied on consent: consent of every single trust in England had to be obtained to secure partnerships with the state. This is what triggered the practice of issuing directions, that is, orders under secondary legislation to facilitate cooperation between the NHS and GCHQ. A remaining question is whether existing legislation ought to be amended to provide for implied consent or whether the practice of issuing directions can be maintained.

The final part of the presentation focused on the UK approach to attribution, including its work with international partners. It was clarified that, while it is often lamented that attribution is incredibly complex and near impossible to achieve, **state organs are capable of retracing the steps of cyber operations to their**

perpetrators. Working with partners can speed up this process. **International law plays a key role, as it gives a common language for discussing substantive thresholds and evidentiary standards.**



International law plays a key role, as it gives a common language for discussing substantive thresholds and evidentiary standards.



Presentation 3

Philip Howard

Director of the Oxford Internet
Institute

Photo: WHO-openaccess

The third presentation centred on the trends in misinformation and disinformation in their relation to the emergence of Covid-19 and the vaccines under trial. According to Professor Howard, two interesting developments could be discerned. A first development was the arrival of China as a superpower in generating disinformation. Its disinformation operations are varied in their targets, but a significant portion is directed at the democracy movement in Hong Kong and Covid-19. It is becoming clear that China cares about perceptions in the West: their content is in English and the addressees are individuals living in the West. This style of disinformation operations differs from that of Russia. Russia's approach is to create a network of long-term characters with multiple social media accounts. These characters may start by posting about soap operas and flowers, slowly reorienting themselves to politics. This, in turn, makes them harder to catch.

The Chinese way, on the other hand, relies on the sheer volume of fake accounts, and the connections between these accounts. Given the volume of accounts, when content is created and pushed across networks, it can go across the human barrier.

Some key messages permeate the content pushed by China and Russia. Democracies are weak and failing, and they are incapable of taking quick and important decisions. Democratic leaders are soft. China and Russia are leading in science and humanitarian assistance.

The speaker detailed the nature of a complex ecosystem that comprises the White House under Trump, white supremacists and ultra-conservatives in the US, and Russian and Chinese-generated disinformation. Very often, Russian and Chinese content will only ask leading questions: for instance, 'did Covid-19



The creation and spread of disinformation occur within a complex ecosystem of interactions.

originate in a plant in Colorado?’ They are also successful in linking the long-standing anti-vax campaign with the fear of Bill Gates, 5G, chips and other conspiracy theories. **The package of stories is incredibly complex and has a lot of resilience to it.**

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



Presentation 4

Talita Dias

Postdoctoral Research Fellow,
ELAC

Photo: John Cairns/Oxford Biomedical Research Centre

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

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

Turning to the first point, the cyber due diligence toolkit comprises measures that ought to be adopted at all stages of the development of the vaccine.

All development stages are essential for the vaccine to be produced and distributed to the population, and all these stages are highly dependent on

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

The second point was directed at



Regardless of whether there is a general rule of due diligence under international law, there is already a set of primary rules containing a due diligence standard that require the protection of vaccine research.

emphasising that, regardless of whether there is a general rule of due diligence under international law, there is already a set of primary rules that require the protection of vaccine research by states. These obligations overlap in some respects, as they require the taking of measures to prevent, halt and redress certain conduct and/or harm. Four categories of obligations were examined in more detail: the Corfu Channel principle, the no-harm principle, positive duties arising under international human rights law (for instance, under the rights to life, health, property, bodily integrity), and obligations under international humanitarian law.

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

states are under an obligation to ensure a baseline of protective capacity.

Session II: Open discussion



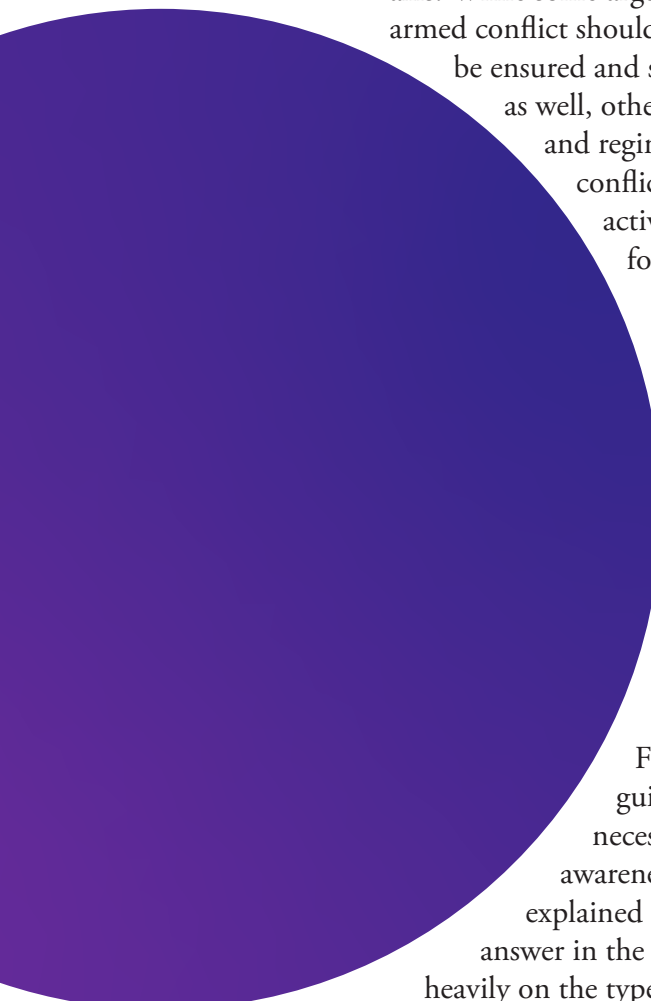
Moderator:
Prof Duncan Hollis
Temple University

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

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

information contained therein on the way in or on the way out.

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



international law provides along the peacetime/armed conflict axis. While some argued that the protections under the law of armed conflict should be seen as the bare minimum that must be ensured and should consequently apply in peacetime as well, others emphasised the need to keep the rules and regimes separate, since the law of armed conflict provides specific protections of medical activities that do not exist, in this specific form, in peacetime.

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

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

Sixth and finally, it was also queried whether certain types of espionage could actually be considered beneficial

– when done with care and contributing to the speedy development of vaccines. In this sense, some participants proposed the disaggregation of confidentiality, integrity and availability, with integrity and availability taking centre stage and confidentiality receding to the status of a secondary consideration. Others disagreed, arguing that **unpacking confidentiality without impacting integrity and availability may be impossible.** To get past any form of protection, one must do something, and that something can cause damage. The practice of the Jenner Institute at Oxford was highlighted, as their approach of making their work as transparent and accessible as possible could help reduce the number of operations seeking to breach their cyber defences.

Concluding remarks

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

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

Why now? International law has a role to play in protecting vaccine research, production and distribution. Its role is

becoming increasingly critical at a time of intensifying cyber operations against institutions engaged in the development of Covid-19 vaccines. This is why the Oxford Process can step in and produce Statements that, in a clear and concise way, outline the applicable international legal rules and how they apply to particular objects of protection.

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

List of Participants

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

List of Participants

25. **Henning Lahmann**, Senior Researcher, Digital Society Institute, ESMT Berlin
26. **Nemanja Malisevic**, Director, Digital Diplomacy International Lead, Defending Democracy Program, Microsoft
27. **Suzuki Masaru**, First Secretary, Embassy of Japan in the United Kingdom
28. **Tomohiro Mikanagi**, Deputy Director-General of the International Legal Affairs Bureau, Ministry of Foreign Affairs of Japan
29. **Tomáš Minárik**, Head of International Organisations and Law Unit, National Cyber and Information Security Agency of the Czech Republic
30. **Harriet Moynihan**, Senior Research Fellow, International Law Programme, Chatham House
31. **Jan Neutze**, Senior Director, Digital Diplomacy, Microsoft
32. **Jim O'Brien, Vice Chair**, Albright Stonebridge Group
33. **Michael Pinhorn**, Head of Security Governance, Risk and Compliance, Information Security Team (InfoSec), University of Oxford
34. **Daniela Rakhlina-Powsner**, JD Candidate, Temple University
35. **Przemysław Roguski**, Lecturer in Law, Jagiellonian University in Kraków
36. **Michael Schmitt**, Professor of Public International Law, University of Reading
37. **Nikhil Sud**, Regulatory Affairs Specialist, Albright Stonebridge Group
38. **Wieteke Theeuwes**, Legal Officer, Ministry of Foreign Affairs of The Netherlands
39. **Tsvetelina van Benthem**, DPhil Candidate in Public International Law, University of Oxford
40. **Liis Vihul**, Chief Executive Officer, Cyber Law International
41. **Doug W**, GCHQ
42. **José Singer Weisinger**, Permanent Representative of the Dominican Republic to the United Nations
43. **Nathalie Weizmann**, Senior Legal Officer with the UN Office for the Coordination of Humanitarian Affairs
44. **Briony Daley Whitworth**, Assistant Director, Cyber Affairs Branch, Department of Foreign Affairs and Trade, Australia
45. **Elizabeth Wilmshurst**, Distinguished Fellow, International Law Programme, Chatham House
46. **Robert Young**, Legal Counsel, Global Affairs Canada

OXFORD INSTITUTE FOR ETHICS, LAW AND ARMED CONFLICT



OXFORD INSTITUTE FOR
ETHICS, LAW AND
ARMED CONFLICT



THE
OXFORD
PROCESS