THE OXFORD PROCESS

BLAVATNIK SCHOOL OF GOVERNMENT
UNIVERSITY OF OXFORD
OXFORD INSTITUTE FOR ETHICS, LAW AND ARMED CONFLICT

21 July 2022

ELAC Intervention

United Nations Open-ended Working Group on security of and in the use of information and communications technologies (OEWG)

Third Substantive Session

Good afternoon, Mr Chair, and esteemed Delegates,

My name is Talita Dias and today I am speaking on behalf of the Oxford Institute for Ethics, Law and Armed Conflict ('ELAC'). Before anything, we would like to express our deep regret at the veto to our accreditation request to attend the formal meetings of this Third Substantive Open-ended Working Group on security of and in the use of information and communications technologies (OEWG). We are a politically neutral academic institution that prides itself on its global membership and engagement. We are also sorry that other stakeholders received objections to their accreditation requests. We believe our contribution to fostering international peace and security in the field of ICTs would be most effective if we were all allowed a seat at the stakeholder table.

**

On stakeholder involvement in capacity-building

As an **academic institution** bringing together leading international lawyers, we have spared no effort to build the **legal capacity** of States on the **application of international law to ICTs**. We have done so primarily by hosting several **expert meetings and workshops** that seek to bring together representatives of States and international organizations, academics, NGOs and civil society in the context of the so-called Oxford Process on International Law Protections in Cyberspace. These discussions have been extremely fruitful, leading to several concrete outputs. The most important among these are our Five Oxford Statements on International Law Protections in Cyberspace. Our publications also include reports of the discussions held during expert workshops, as well as blog posts, op-eds and articles on discrete topics relating to the application of international law in cyberspace. We have also offered tailored **lectures, seminars, and talks** to representatives of a range of member States. The **results** of our capacity-building work can be seen in references to the Oxford Process and its various Statements in pronouncements and documents issued by States, international organizations, and stakeholders over the past couple of years.

In discussions with member States, we have found it crucial to **listen to their particular needs** and take into account their **distinct views on international law** and its application to ICTs. We not only

share knowledge but **exchange it**, empowering States to have their **own voice** in this arena. We are confident that this model of capacity-building has the potential to bridge divides that still exist between States on core issues relating to the application of international law to ICTs.

**

On how stakeholders can work together with States to contribute to the implementation of the concrete, action-oriented proposals made by States at the first and second substantive sessions of the OEWG

In response to the Chair's **first question** in this regard, we make **two suggestions** on the Zero Draft Annual Progress Report's action-oriented proposals on **international law**.

First, we think that stakeholders, particularly academia, can meaningfully contribute to the proposed OEWG-convened **discussions on specific topics related to international law**. As we noted earlier, our ongoing work within the Oxford Process has already made an important contribution to our understanding of **how international law applies to ICTs**. Notably, we have helped to clarify that **existing international law as a whole** applies to these technologies, without it being strictly necessary to identify new rules of customary international law or craft new treaty instruments to regulate State behaviour in cyberspace. This is a crucial step in any discussion on what exact rules of international law are applicable and relevant to ICTs, such as sovereignty and due diligence. We also think that a helpful way to advance discussions in this area is by focussing on issues where **common ground** among member States can be found. For example, while there is controversy as to whether sovereignty is a separate rule of international law applicable to ICTs, there is **consensus that certain types of cyber operations such as cyberattacks against the healthcare sector are prohibited by international law**, either because of their methods or effects. Thus, we believe that future discussions about how international law applies to ICTs should prioritise instances of **prohibited, permitted, and required State behaviour**, without necessarily delving into existential or theoretical debates about distinct international legal rules.

Second, we believe that stakeholders, including academia and the industry, can play a crucial role in advancing member States' understanding of **what international law actually requires from States in different circumstances.** Discussions about the **actual implementation of international obligations in cyberspace** can dispel doubts about the feasibility of and compliance with those rules. Such discussions should cover the various **technical, legal, and institutional measures** that are available to different States in discharging their international legal obligations. This could greatly benefit from States' sharing of **best practices** at the international, regional, sub-regional and national levels. But it also requires a **more meaningful dialogue between international lawyers, policymakers, and technical experts.**

In response to the Chair's **second question on specific proposals that can be expanded** to cover stakeholder groups, we believe that **both the international law discussions and legal capacity-building efforts** proposed in the Zero Draft Annual Progress Report should be **expanded to include stakeholders** other than the international and regional organizations mentioned in the report. As we have already noted, a comprehensive understanding of how international law applies to ICTs necessitates **different perspectives**. This includes representatives of **academia, civil society, and the industry** with expertise not only in **international law but also in cybersecurity and public policy.**

We thank the Chair for this opportunity to share our views and we look forward to our continued participation in the OEWG.

Thank you.