PERMANENT MISSION
OF THE PRINCIPALITY OF LIECHTENSTEIN
TO THE UNITED NATIONS
NEW YORK

NEW YORK, 10 FEBRUARY 2020 CHECK AGAINST DELIVERY

OEWG ON DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY

INTERNATIONAL LAW

STATEMENT BY GEORG SPARBER, DEPUTY PERMANENT REPRESENTATIVE

PERMANENT MISSION OF THE PRINCIPALITY OF LIECHTENSTEIN TO THE UN

Mr. Chair,

Before entering into the subject matter, Liechtenstein would like to thank you for your continued leadership in the Open-Ended Working Group. Halfway through its mandate it is obvious that the Working Group has already significantly advanced our collective understanding and brought useful and in-depth exchanges between States as well as with civil society actors. The intersessional consultations with civil society have been rich and instrumental to States in their efforts to determine the framework for an open, free, stable and secure cyberspace. It is particularly anachronistic that civil society actors continue to be restricted from participating in our discussions, in an area where they are often at the vanguard of technical innovation and can bring unique perspectives on issues such as current and future trends, specific vulnerabilities or human rights and development aspects of digitization. States that oppose the participation of all relevant actors deliberately deprive themselves and others from the best available knowledge base for our decision-making. For future discussions on cybersecurity at the United Nations to be meaningful, we cannot afford such an overly restrictive mandate for the engagement with civil society, in particular as we witness to what extent it will be abused to limit our discussions.

Mr. Chair,

As we begin deliberations on the product of this Working Group, we should be guided by the ambition to cover the breadth and depth of our exchanges here, building on the understandings that we have already achieved. The key point of departure is the recognition that cyberspace is not a lawless environment, neither for States, nor for individual actors. Quite to the contrary: Following the endorsement by the international community of consecutive reports by the Group of Governmental Experts, there can be no question that cyberspace is already governed by international law, including the UN Charter in its entirety and other bodies of international law, in particular in the areas of international humanitarian law, human rights law and international criminal law.

Currently the international community relies mostly on analogy and customary international law to regulate cyber behavior. This, however, is not good enough. There is a need to concretely identify specific international law addressing current and emerging threats emanating from cyberspace and to propose sensible interpretations that will build on existing legal foundations to ensure clarity in the application of the law in the cyber age.

As we witness concerning trends towards an increasingly militarized cyberspace, unchecked applications of artificial intelligence, pervasive data collection and manipulation, as well as highly sophisticated or large-scale cybercrime, we have to consider these as real security risks to States and their citizens. But we also have to consider them as they affect the other pillars of the United Nations' work: human rights and sustainable development. These trends therefore need to be analyzed thoroughly against the existing normative framework and addressed comprehensively at the United Nations.

Mr. Chair,

Developments in the cyber realm require us to align international criminal justice with 21st century challenges. In this regard, Liechtenstein together with partnering States has convened a

Council of Advisers, composed of leading academics, to elaborate how the Rome Statute of the International Criminal Court in particular applies to cyberwarfare. Having a clear understanding of Rome Statute application in place will act as an important deterrent to malicious cyber-operations and will contribute to ensuring accountability for acts of cyber-aggression. Understanding how the Rome Statute applies in the cyber context will also complement the work of the OEWG and the GGE.

It can also help to guide the development of investigations and prosecutions of these crimes in the future. Attribution is not only important with regard to state responsibility, but also for individual criminal accountability. Given difficulties with regard to attribution in the cyber realm, we are also looking favorably at the possibility of a robust global attribution framework that can complement the work of existing national and international courts.

We want to flag the issue of the relevance of international criminal law here as it is of obvious relevance for the work of the OEWG, while we will not pursue the substance of discussions here at this time.

Thank you