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

NEW YORK, 14 DECEMBER 2021 CHECK AGAINST DELIVERY

OEWG ON SECURITY OF AND IN THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES 2021–2025

GENERAL EXCHANGE OF VIEWS

STATEMENT BY H.E. MR. CHRISTIAN WENAWESER

PERMANENT REPRESENTATIVE OF THE PRINCIPALITY OF LIECHTENSTEIN TO THE UN

Mr. Chair,

Our congratulations on the assumption of the chairmanship of the OEWG. We will fully support you in your task. We also want to extend our gratitude to Ambassador Lauber for his excellent stewardship during the previous phase of our work. We are thankful for your thorough preparation, as well as that of the secretariat, which will hopefully set the stage for a constructive and informed dialogue.

The OEWG provides an inclusive multilateral format where work on aspects of ICT and security policy can come together, including those in regional organizations such as the OSCE, initiatives among other groups of States as well as the private sector and civil society. One further potential strand is the initiative for a Programme of Action, which we support and consider an alternative to advance cyber security that can be commensurate to the aspiration to make tangible progress towards compliance with international law and increased collective security. We commit to sustain an inclusive dialogue with all relevant stakeholders to that effect.

Mr. Chair,

The OEWG should adopt a targeted approach, which clearly places the question of cyber security into the context of the United Nations' core mission to advance peace and security, human rights and sustainable development. Trends towards an increasingly militarized cyberspace, developments in artificial intelligence, pervasive data collection and manipulation, as well as cybercrime constitute real security risks to States and their citizens. They need to be analyzed thoroughly against the existing legal framework and addressed comprehensively across all three pillars of the United Nations' work.

Human rights have long been recognized by all States as a legitimate concern of the international community and a priority for the United Nations. That recognition also constitutes a responsibility for the OEWG to contribute to the implementation of established human rights obligations in cyberspace, including the right to privacy, freedom of expression, and freedom of information. Our constituents will also look at the OEWG as a forum to contribute to narrowing digital divides and tap the potential of ICTs for sustainable development and inclusive societies globally.

Mr. Chair,

The previous report of the OEWG reaffirms the acquis of past agreements. But it could do more to reflect how exactly cyberspace is governed by international law, including international humanitarian law and international criminal law. The obvious problem of ensuring accountability for violations of international law in cyberspace, both from a perspective of State and individual criminal responsibility, and the inherent challenges of attribution linked to it, are largely missing from the report. Liechtenstein reiterates its position that it sees no need to elaborate additional legal obligations in the framework of legally binding instruments. Rather, our discussions on how to apply existing international law must advance.

Mr. Chair,

One of the most pertinent questions with respect to international law is indeed its application to

cyberspace. Liechtenstein underscores the importance of upholding the rules-based international order and international law in cyberspace and sees a key role for the OEWG in the promotion of peace and stability in cyberspace.

Modern warfare has an inextricable cyber dimension. Grave cyberattacks can result in the closure of hospitals, infrastructure, power grids, industries, and result in massive civilian casualties. We need to address such challenges collectively and look at both practical and legal challenges arising thereof. The strengthening of norms, rules, and principles on the responsible behavior of States in cyberspace will play a key role in this regard, based on previous agreements within the UN and other bodies. We need to urgently develop a framework to harmonize international law in this area, including the expansion of the fight against impunity to the cyber domain. International criminal law and in particular the Rome Statute of the ICC must be included in these analyses.

Together with ten other State Parties to the Rome Statute, we have created a Council of Advisers that helped produce an in-depth report of the application of the Rome Statute to cyber warfare. The Council of Advisers reached the unanimous conclusion that the Rome Statute's provisions indeed apply to cyber warfare – without the need for statutory amendment. While we realize of course that a good number of States have not joined the Rome Statute at this time, the provisions of the Rome Statute defining the core crimes are largely drawn from existing treaties that are very widely ratified or else negotiated with universal participation. Liechtenstein will place a particular emphasis on this question as a contribution to the work of the OEWG and looks forward to fruitful exchanges on this and other topics in future meetings.

I thank you.