



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

---

NEW YORK, 9 SEPTEMBER 2019

CHECK AGAINST DELIVERY

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

**GENERAL EXCHANGE OF VIEWS**

**STATEMENT BY H.E. AMBASSADOR CHRISTIAN WENAWESER**

PERMANENT REPRESENTATIVE OF THE PRINCIPALITY OF LIECHTENSTEIN TO THE UN

Mr. Chair,

Congratulations to you on the assumption of the chairmanship of the OEWG. I assure you that you will find in the Liechtenstein delegation a strong supporter of your efforts to broaden and deepen our understanding and our joint commitments in the area of cyber security. We are grateful for the thorough preparations from your side and from the secretariat that will make for very interesting discussions in the days to come and hopefully set the stage for a constructive and informed dialogue among States, experts and civil society in the framework of the OEWG.

Cyber security has become a top priority for many if not all of our governments and it is a topic where the UN should rightfully play a leading role – we are grateful to the Secretary-General and the High Representative for their continued high ambition in that respect. Our engagement as States in this OEWG should live up to that ambition. We are hopeful that broad common interest in a strengthened rule of law in cyberspace will drive future discussions.

Mr. Chair,

The OEWG provides an inclusive multilateral format where different strands of work on different aspects of ICT and security policy can come together. This includes the work undertaken in the Group of Governmental Experts (GGE), in regional organizations such as the OSCE, initiatives among other groups of States as well as the private sector and civil society. It will thus be important to allow for broad participation, in particular also from civil society, and to contribute to the complementarity of efforts among intergovernmental bodies.

Liechtenstein is of the view that the OEWG should adopt a targeted approach to its mandate, which clearly places the question of cyber security into the context of the United Nation's 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.

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 by States in cyberspace, including the right to privacy, the freedom of expression, and the 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. Last, but not least, we are all keenly aware that the future of warfare has an inextricable cyber dimension. We will have to 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.

Mr. Chair,

Following the endorsement by the international community of consecutive reports by the GGE, including its 2015 report, 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. We should now build on what has already been agreed, and avoid undermining important progress that has already been achieved. The OEWG should help to advance the implementation of previously agreed rules, norms and principles of responsible State behavior, and further delineate how international law applies to cyberspace.

Mr. Chair,

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. 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. Developments in the cyber realm also require us to better align international criminal justice with 21st century challenges. Currently we rely mostly on analogy and customary international law to regulate cyber behavior. There is however a need to concretely identify specific international law addressing current and emerging threats emanating from cyberspace and to propose sensible interpretations that will update the law for the coming age in order to ensure its relevance in cyberspace. 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. With the increasing digitization of warfare, understanding the extent to which the Rome Statute and other international legal frameworks apply to cyberattacks and cyber warfare is imperative. 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 the coming week and months. Thank you.