Contribution to the First Substantive Session of the Open-Ended Working Group on the security of and in the use of information and communications technologies 2021-2025 (OEWG)

Contribution by DiploFoundation

10 December 2021

In response to the invitation by the Chair of the Open-Ended Working Group on the security of and in the use of information and communications technologies 2021-2025 (OEWG) to interested, non-governmental stakeholders to share their views on the topics under consideration by the OEWG, DiploFoundation hereby provides its contribution to the first substantive session of the OEWG.

The following contribution provides messages from the work of the Geneva Dialogue on Responsible Behaviour in Cyberspace, an initiative led by the Swiss Federal Department of Foreign Affairs (FDFA) and implemented by DiploFoundation. Geneva Dialogue shapes a joint vision regarding the security of digital products with leading industries, and enhances their understanding of and contribution to global policy processes in order to achieve a trusted, secure, and stable cyberspace. More information about the Geneva Dialogue is available in the Annex, and at [https://genevadialogue.ch/](https://genevadialogue.ch/).

This contribution aims to support the work of the OEWG by providing suggestions related to reducing the vulnerabilities and preventing their exploitation, and by underlining the important role the industry and non-government actors have to play in this regard.

DiploFoundation and the Geneva Dialogue remain available for additional inputs, as well as for new partnerships in this field.
Firstly, we call for an open, inclusive, and transparent OEWG, with contributions by all the interested stakeholders.

In order to be able to implement the framework of responsible behaviour – both the provisions of the current acquis and those in the future – we need 'all hands on deck'. We need all the stakeholders to play their roles and take their responsibilities, while feeling the ownership of the framework; this, in turn, requires their full involvement in all phases of the process, including the shaping of the outcomes. We are confident that, under the leadership of Singapore which has already set the example of an inclusive dialogue in 2020, this OEWG will make further steps forward.

To provide a systemic basis, OEWG should embed inclusiveness of all stakeholders into the fabric of the future institutional dialogue.

Secondly, we call for a public recognition of exploitation of vulnerabilities as one of the most concerning among the emerging threats, and invite states to restrain from, and prevent exploitation of vulnerabilities.

Vast majority of sophisticated high-impact cyber attacks exploit one or more vulnerabilities in our digital environment – often those not even known to the producers (known as zero-days). Exploitation of vulnerabilities for commercial purposes, deployed in the interest of politics – as we have witnessed in the case of the NSO Group and Pegasus – further increases the stakes. Exploitation of vulnerabilities undermines the very concept of digital society, on which we rely more than ever in times of COVID-19 pandemic. By reducing vulnerabilities and their exploitation, we can significantly increase the costs of cyber attacks and reduce their volume.

An important milestone will be for the OEWG to clearly condemn exploitation of vulnerabilities for criminal, commercial, and political purposes.

Thirdly, we call for greater transparency and responsibility of states in relation to collecting and exploiting vulnerabilities.

Following on concerns related to states increasingly developing their offensive cyber capabilities, expressed also by the GGE and OEWG in 2021, it is essential that states show responsibility in providing transparency about the type of capabilities and procedures of their deployment. Such transparency should ensure greater predictability, and reduce likelihood of severe global effects of vulnerability exploitation.
Fourthly, we call on states to cooperate with the industry and other stakeholders when developing favourable national regulatory frameworks to prevent the emergence and exploitation of vulnerabilities.

Adopted framework of responsible state behaviour in cyberspace calls upon governments to encourage measures to
- ensure safety and security of ICT products throughout their lifecycle (norm 13(g)),
- ensure supply chain security including through developing national regulatory frameworks and adopting cooperative measures (norm 13(i)),
- report ICT vulnerabilities, including through putting in place legal frameworks against exploitation, and developing processes for responsible vulnerability disclosure (norm 13(j)).

The industry, along with standardisation and technical communities and other stakeholders, plays a crucial role in efficient implementation of these measures. National regulatory framework should, therefore, take into consideration not just global norms and principles, but especially the industry good practices, international standards developed by the standardisation organisations and communities, and efforts by the academia, technical community, and the civil society on creating more secure digital products.

The OEWG should provide further guidelines on the main principles and cooperation mechanisms to achieve favourable and harmonised regulatory environment in this field, not least following the work of the Geneva Dialogue on Responsible Behaviour in Cyberspace. Detailed analysis of the challenges with, and guidelines for developing national regulatory frameworks for security of digital products are available in Annex I.

Finally, we emphasise the need for greater capacity building efforts to strengthen the security of digital products, and reduce vulnerabilities.

Diplomats require additional support to understand the origins of vulnerabilities, geopolitical and economic risks of their exploitation, and challenges related to securing the interconnected environment. Regulators require further capacities to model national frameworks in a meaningful and effective manner, taking into consideration global norms, industry practices, and standards. On the other hand, the industry, as well as standardisation and technical communities and civil society, require support to better connect their practical work with global norms and principles, and meaningfully contribute to international negotiations and national regulatory processes.

Building on the capacity building principles elaborated by the OEWG and GGE in 2021, OEWG should invite for a more comprehensive and inclusive capacity building, which connects global norms and principles with the regulatory environment and good practices of non-state actors.
Annex – Related Geneva Dialogue resources

The Geneva Dialogue on Responsible Behaviour in Cyberspace, led by the Swiss Federal Department of Foreign Affairs (FDFA), and implemented by DiploFoundation, helps shape a joint vision regarding the security of digital products with leading businesses, and enhances their understanding of and contribution to global policy processes to achieve a trusted, secure, and stable cyberspace. Building on its ground-breaking work, most notably the collection of good industry practices, the Geneva Dialogue endeavours to enhance the feedback loop between corporate efforts and cybersecurity processes that develop norms, regulations, policies, and standards.

Geneva Dialogue partners are leading companies with are concerned with security of digital products: ABB, BI.ZONE, CISCO, Cognizant, CyberCX, EnSign, FireEye Mandiant, Huawei, Kaspersky, Microsoft, NCR, PNG ICT Cluster, Siemens, SICPA, SwissRe, TCS, TechMahindra, VU, Wipro, WiseKey, and UBS.

Through its broad deliberations among leading industries with key standardisation organisations, and number of national regulators and representatives of governments, Geneva Dialogue has produced valuable resources related to security of digital products, and reducing vulnerabilities of the connected environment in general:

- Collection of working definitions and good industry practices: ‘Security of digital products and services: Reducing vulnerabilities and secure design - Good practices’ (2020)
- Report with key findings from the event: ‘Security of digital products and international standards’ (2021)
- Report with key findings from the event: ‘Security of digital products and the regulatory environment’ (2021)
- Research conducted by the ETHZ CSS: ‘Governance Approaches to the security of digital products’ (2021)