DiploFoundation

Open-Ended Working Group on the security of and in the use of information and communications technologies 2021–2025 (OEWG)

Informal dialogue

Statement by DiploFoundation

28 February 2024

Mr. Chair, distinguished delegates, and colleagues,

My name is Anastasiya Kazakova. I represent DiploFoundation, a nonprofit educational organisation supporting small and developing countries, as well as various stakeholders in industry and civil society through capacity building in cyber diplomacy, cybersecurity and internet governance topics for over 20 years.

Mr. Chair, we would like to express our further support for the work of the OEWG. ***Regarding your question on the roles stakeholders could take to support the implementation of the norms,*** Diplo is happy to share the results achieved by the Geneva Dialogue on Responsible Behaviour in Cyberspace. Established by Switzerland and led by DiploFoundation, it focuses on the roles and responsibilities of non-state stakeholders in the implementation of agreed norms. The Geneva Dialogue brought together over 50 representatives and independent experts from the private sector, civil society, academia, and technical community and developed the first chapter of the Geneva Manual. It is a comprehensive guide on the implementation of two UN GGE norms I and J, related to ICT supply chain security and responsible reporting of ICT vulnerabilities by relevant non-state stakeholders.

The Manual draws from multistakeholder inputs and provides valuable insights to the OEWG, addressing implementation challenges, showcasing good practices, and outlining stakeholder expectations from each other and states. It raises stakeholder awareness of the normative framework and identifies areas requiring further discussions at various levels.

It also identified challenges with regard to norms I and J. In particular, emerging cybersecurity regulations should avoid requirements to mandate reporting of unpatched vulnerabilities to anyone else but to code owners in order to minimise the risks of malicious

Geneva	7bis, avenue de la Paix, 1202 Geneva 2, Switzerland | *t.* +41 22 741 0420, *f.* +41 22 731 1663
Malta	5, Hriereb Street, Msida, MSD 1675, Malta | *t.* +356 21 333 323, *f.* +356 27 333 323
Belgrade	Braničevska 12a, 11000 Beograd, Serbia | *t.* +381 11 3230 291, *f.* +381 11 3063 323
Washington DC	1100 15th St NW, FL 4, 20005 Washington, DC, USA | *t.* +1 202 834 4946

actors accessing this information. Active engagement with the open-source software community is crucial for implementing these norms. Implementing the two norms requires practical actions, including policies and regulations. A neutral and geopolitics-free governance framework is required to approach the security of ICT supply chains globally, the responsible reporting of ICT vulnerabilities, and the security of digital products. While this may be an ambitious goal, international dialogue is critical across different jurisdictions involving industry, independent developers, SMEs, cybersecurity researchers, and technical community members who contribute to responsible vulnerability disclosure.

The first chapter of the Manual is available on the OEWG webpage at:https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Geneva_Manual_On_Responsible_Behaviour_in_Cyberspace_Geneva_Dialogue.pdf

In the immediate future, the Geneva Dialogue will focus on studying norms and CBMs related to critical infrastructure protection. We welcome interested stakeholders to participate.

Thank you for this opportunity, Mr. Chair.