DiPLO
DiploFoundation

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

Informal dialogue with relevant stakeholders

Contribution by DiploFoundation

11 July 2023

Mr. Chair, distinguished delegates, and colleagues,

My name is Pavlina Ittelson. I will be speaking on behalf of DiploFoundation, a nonprofit organisation that for more than 20 years has provided capacity building to support small and developing countries to represent themselves and to meaningfully contribute to international discussions. Over the years, Diplo has provided neutral, impartial capacity building in internet governance and cyber-related topics to almost all countries worldwide, as well as international and regional organisations, and representatives of relevant stakeholder groups.

Mr. Chair, we would like to express our appreciation for your continual efforts to ensure the participation of all interested stakeholders in the work of the OEWG, including today's session. Diplo is also pleased to further support the work of the OEWG 2021–2025 by sharing today the ideas on how stakeholders can work together with states to contribute to the implementation of the proposals captured in the zero draft of the second annual progress report (APR).

We will reflect on such proposals with ideas based on our expertise as a capacity development nonprofit, as well as based on regular consultations with representatives of different stakeholder groups (private sector, academia, civil society and technical community) within the Geneva Dialogue on Responsible Behaviour in Cyberspace. The Geneva Dialogue was established in 2018 to map the roles and responsibilities of actors to contribute to greater security and stability in cyberspace. It is led by the Swiss Federal Department of Foreign Affairs (FDFA) and implemented by DiploFoundation, in partnership with the Center for Digital Trust (C4DT).

The **proposal to develop a repository of threats** (as captured in para 15 and 20 of the Zero Draft APR) has the potential to enhance transparency about the ongoing cyber threat landscape and support, at the same time, with practical knowledge to build cyber capacities. In developing this repository, the **OEWG and States can benefit from the vast experience of the non-state stakeholders - the technical community, private sector and civil society in this field**. These stakeholders can supplement the threat-related and threat intelligence information as well as share their action-oriented proposals to address such threats and minimise risks in the event of active exploitation of ICT vulnerabilities and active threats.

The **proposal to encourage the private sector and civil society to play an appropriate role to improve supply chain security for ICT products** (as captured in para 22 (c)) and **elaborate additional guidance on the implementation of norms** (as captured in para 26) are important steps forward to the operationalisation of the agreed framework. We also support a proposal to **convene an informal intersessional meeting** (as captured in para 27) **with the participation of relevant experts, including businesses, NGOs, and academia**. Geneva Dialogue participating stakeholders acknowledged that implementing the agreed norms and, in particular, securing ICT supply chains is a shared responsibility. At the same time, some open questions have been voiced, which we would like to share as possible areas to advance the implementation of the norms:

- Cybersecurity is often added too late in ICT development; therefore, manufacturers need to develop and implement an **interoperable minimum set of baseline security requirements**. However, stakeholders shared concerns about the risk of further fragmentation in regulating cybersecurity in ICT products and services.
- Security of ICT supply chains and effective response to supply chain vulnerabilities requires **greater transparency and visibility in software composition and regular security assessments of all third-party components, including from open-source**. Certifications and security ratings are mentioned as possible solutions in this regard. However, a lack of cybersecurity talent and capacities for regular security testing has also been mentioned as a challenge.
- Participants in the Geneva Dialogue stressed the importance of **cross-border and cross-sector cooperation to exchange relevant vulnerability information** with international partners, for example, through FIRST, regional or bilateral channels for implementing the norm related to responsible reporting of ICT vulnerabilities. At the same time, where CERTs/CSIRTs or national government agencies are parts of such cooperation, greater transparency from government processes and rules for vulnerability treatment and disclosure seem crucial to ensure trust and security.
- Civil society and academia’s contributions **can play a vital role in raising awareness and engaging in dialogue with businesses on behalf of ICT end users, demanding greater security in ICT products and services**. However, the lack of expertise was reiterated, emphasising the challenge and importance of capacity building for civil society and academia.

Mr. Chair, these are some of the outputs of the continual multistakeholder consultations within the Geneva Dialogue, and we aim to produce the Geneva Manual, a comprehensive guidance to support relevant stakeholders with the implementation of the norms related to responsible reporting of ICT vulnerabilities and supply chain security; Geneva Manual will contribute directly to the implementation of the agreed norms by all stakeholders. Once it is finalised, we will be happy to share the results with the OEWG and stakeholders.

Mr. Chair, the request to the UN Secretariat to **conduct a mapping exercise about capacity building programmes and initiatives globally** and to **produce a report with the findings** (as captured in para 43), as well as the request to the OEWG Chair to **convene a dedicated Global Roundtable meeting** in this regard are extremely important and positive steps to improve coordination in capacity building. As mentioned in our previous interventions and contributions, Diplo strongly supports such mapping to ensure a holistic approach to capacity building, appropriate capacity building methodologies, and the cross-pollination of knowledge and experience across thematic and organisational silos. It is vital that the OEWG does not duplicate the role of any existing regional and global capacity building mechanisms and programmes, but rather enhances their outreach to local partners and beneficiaries, and assists with better coordination of donors and implementers.

Since non-state actors play an important role in comprehensive capacity building, we believe that **relevant stakeholders should also be allowed to contribute to the mapping exercise and share the examples and results of their work in this field**. Limitations on stakeholder participation or topics that the stakeholders can provide their inputs on would result in incomplete and unbalanced information being available to states and, in some cases, affect states' ability to negotiate effectively for their aims. This particularly impacts small and developing states and those with the greatest need for capacity building in ICT security.

Diplo fully supports the UN Secretariat in this initiative, and is available to contribute to these important efforts, including by sharing the information about ongoing capacity building programmes and initiatives, based on more than 20 years of experience.

Thank you for this opportunity, Mr. Chair.