kaspersky

Virtual Informal Dialogue of the 2021–2025 UN Open-Ended Working Group (OEWG) on developments in the field of information and telecommunications (ICTs) in the context of international security and peace

Kaspersky's Statement

March 24, 2022

Mr. Chairman, dear all,

Kaspersky supports the UN OEWG's efforts to promote international cooperation and peace in cyberspace. We supported the previous UN OEWG by sharing the expertise of our cybersecurity specialists, and we also shared eight practical suggestions, from a cybersecurity research perspective, after the First Substantive Session of the new UN OEWG. In line with this submission, we are grateful to share today our input regarding the items in the Chair's letter.

Existing and potential threats in the sphere of ICT security

1. The international community needs greater acknowledgement of the critical issue of vulnerabilities in modern ICTs as entry points for cyberattacks, which did not receive a thorough discussion in the recently agreed UN OEWG and GGE reports. In this regard, we also call for:
    - greater transparency and responsibility by both States and non-state actors in the vulnerability treatment, including their discovery, reporting and stockpiling; and
    - further promotion, on a global scale, of clear processes for responsible vulnerability reporting and disclosure.

    Fortunately, many good practices already exist – such as those developed by the Geneva Dialogue, FIRST, OECD, and the larger CERT/CSIRT community, and they could guide further developments in this regard.

2. The international community needs to identify and protect, in a global coordinated action, broadly-used critical open-source software technology, which also compose the public core of the internet infrastructure. The recent disclosure of a series of vulnerabilities in open source libraries (log4j) highlighted the "endemic vulnerability" across the global internet within old and new software products, thus affecting multiple stakeholders in the software development community, tech industry and government.

    There should be global coordinated efforts to ensure the availability and security of these critical open source tools and libraries, as they are critical for conducting in-depth assessment and vulnerability research.

3. For effective critical infrastructure protection and ICT supply chain security, we also call for enhancing interoperability and harmonization of national regulatory practices.

kaspersky

As the risk of fragmented approaches across States, jurisdictions and sectors to develop such tools and regulate the security of (as of now, at least) globally developed, distributed, and consumed ICTs poses a threat, it could potentially lead to greater insecurity. In particular, there is a growing risk of fragmented national approaches to regulate vulnerability disclosure, and we hope that the UN OEWG could be a process to ensure consistency and harmonization in line with existing industry best practices.

Assistance by stakeholders to Member States in implementing the existing rules, norms and principles of responsible state behavior

4. It is important to focus on the implementation of the agreed non-binding norms and confidence-building measures (CBMs) as well as to extend CBMs to relevant stakeholders to develop a global handbook with good practices. Organizing cyber exercises, including with relevant stakeholders and thus extending CBMs to them, to test the operationalizing of the agreed CBMs in a real context could be a possible practice in this regard.

5. It is also important to contribute efforts to ensure a global international cooperation framework for a global cyber incident response in case of significant cyber incidents affecting critical infrastructure located in one or several States. Practically speaking, we call for:
   - establishing and/or identifying national points of contact for coordination and response in case of such significant cyber incidents that can impact international security and peace;
   - standardizing requests for assistance through developing standard operating procedures, which include a template of a request for assistance in order to manage expectations in case of ICT incidents, as well as to agree on a minimum amount of required critical information to be provided in such a request to avoid revealing sensitive information; and
   - ensuring the continuous cooperation between the CERT/CSRIT community and security researchers, despite the political and geopolitical context, as they are essential firemen in protecting users in case of cyber incidents.

6. Especially today it is also important for the international community to clarify the application of international humanitarian law to ensure protections for civilians and civilian infrastructure in cyberspace. In this regard, we applaud and support the work that the International Committee of the Red Cross constantly does to bring more clarity to legal concepts and develop a digital emblem for signaling legal protection during cyberwarfare.

7. Finally, the previously announced suggestions such as the “National Survey of Implementation” could realistically help the international community be better informed about ongoing implementation efforts, and therefore this would help produce effective measures for cyber-stability.

Thank you very much.