kaspersky

Submission to the First Substantive Session of the 2021–2025 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 Position Paper

December 2021

Introduction

Kaspersky supports the UN OEWG and its work aimed at strengthening stability in cyberspace, as well as at promoting international cooperation in this field. We acknowledge the OEWG as a state-driven process and applaud the work by UN Member States to unite global efforts to mitigate the negative impact from the use of ICTs and thus to maintain international security and peace.

At the same time, given the specifics of the cyber context, the inputs and contributions of the multistakeholders (including industry, the technical community, academia and civil society) are vital to ensure that solutions developed to address existing and emerging threats in cyberspace will work and be effectively applied[1].

In this regard, Kaspersky, as a private global cybersecurity company, takes the liberty of providing its suggestions, below, for the 2021–2025 UN OEWG based on its expertise, while also taking into account the valuable work and the UN cyber-stability framework produced by several Groups of Governmental Experts (GGEs). Acting in a good faith, we share our suggestions for the consideration of the distinguished UN OEWG Chair, UN Member States and entire international community.

Suggestions for the 2021–2025 UN OEWG

1. ***Building a multi-speed process with thematic or working groups to effectively deal with multifaceted issues in cyberspace***

   The 2021–2025 UN OEWG should not be an end-goal, but rather an institutional and international process at the UN, which also provides a unique space to discuss the use of ICTs in the context of international security and peace. We believe that the international community should not wait until 2025 to produce meaningful results for stronger cyber-stability. Instead, we need to aim for reaching tangible outcomes already now and throughout the entire five-year process.

   In this regard, the creation of thematic or working groups would allow:

---

[1] In this regard, the Multi-Stakeholder Letter for OEWG Chair on Modalities suggests proposals for modalities for multistakeholder participation and serves an example with practical suggestions. https://letstalkcyber.org/resources/multi-stakeholder-letter-for-oewg-chair-on-modalities

kaspersky

(1) to ensure a multi-speed process (and thus avoid the possibility that the absence of consensus on one particular issue would risk achieving consensus on other issues); and

(2) to coordinate the work of the multistakeholders wishing to contribute to and support interstate negotiations and thus to allow different experts to focus on those thematic or working groups where their expertise could be most relevant. For instance, we at Kaspersky have the expertise and resources to specifically support the operationalization of some non-binding cyber norms (e.g., norms on critical infrastructure protection (norm 13 (g)), ensuring the integrity of supply chains (norm 13 (i)), or responsible reporting of ICT vulnerabilities (norm 13 (j))[2] as well as capacity building).

Thematic or working groups could also be helpful to specifically focus on possible threats stemming from the use of emerging technologies in cyberspace.

2. ***Strengthening further implementation of the agreed non-binding cyber norms and confidence-building measures (CBMs) as well as extending CBMs to relevant stakeholders to develop a global handbook with good practices***

The UN cyber-stability framework agreed on and re-affirmed by all UN Member States is a significant and extremely valuable achievement to guide responsible behavior of actors in cyberspace. We support calls to prioritize further strengthening of the implementation of this framework and specifically its non-binding cyber norms and CBMs, instead of focusing solely on the creation of new ones.

There are some existing tools, such as the UNIDIR Cyber Policy Portal[3], which we find very helpful in understanding better how States implement some norms and CBMs through their legislation, doctrines, strategies and other initiatives. At the same time, the international community needs greater knowledge on how cyber norms and CBMs are practically implemented by both States and relevant non-state actors and where something does not work; which good practices could be used by others; how we could all cooperate and support each other in implementing the framework.

The previously announced suggestions (such as “National Survey of Implementation”[4]) could realistically help the international community be better informed about these aspects, and therefore work further to produce effective measures for cyber-stability.

We have also previously shared our private sector technical perspective[5] to best practice implementation of the 2015 UN GGE norms (A/70/174), and we believe some of the previously discussed ideas in there still have relevance. In particular, developing a common lexicon with consensus-based terminology and definitions related to the use of ICTs could be a good example of the operationalization of norm 13 (a) as well as serve as a confidence-building measure contributing to greater trust and mutual understanding between States.

---

[2] Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, May 2021, https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf

[3] https://unidir.org/cpp/en/

[4] https://front.un-arm.org/wp-content/uploads/2021/02/Joint-Proposal-Survey-of-National-Implementation-FINAL-REV-3-.pdf

[5] https://front.un-arm.org/wp-content/uploads/2020/10/kaspersky-submission-to-oewg.pdf

kaspersky

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 another possible practice in this regard.

3. *Developing a more coordinated global cyber capacity building action which would be inclusive and open to all interested stakeholders to contribute*

We accept the importance of the principles for capacity building agreed in the 2021 UN OEWG consensus report (A/AC.290/2021/CRP.2)[6], and call for a more coordinated global action for cyber capacity building activities and efforts, where the participation of interested stakeholders would take place in a transparent, inclusive and non-discriminatory manner.

We also acknowledge the importance of capacity building action in all these forms: state-to-state, state-to-private, and private-to-private, and we work and will continue working together with other States and multistakeholder community to close the 'capacities' gap. As an example of our capacity building efforts, Kaspersky in cooperation with DiploFoundation has developed the Cyber Stability Games – a virtual exercise and game training to help cyber diplomats, policy and legal researchers as well as all cyber professionals without a technical background to learn the complexities of technical attribution. We have conducted several rounds of such training sessions, including at the UN Internet Governance Forum (IGF)[7], and are happy to provide non-commercial access to the Games further.

4. *Acknowledging the critical issue of vulnerabilities in modern ICTs and developing practical steps to increase our common cyber-resilience in this regard*

Both the recently agreed UN OEWG and GGE reports lack a greater discussion of the critical issue of vulnerabilities in the section on Threats, and they both insufficiently address this issue in further sections on norms and CBMs. Given that vulnerabilities in modern ICTs often serve as an entry point for cyberattacks, we need to pay greater attention to possible practical steps to mitigate these negative security effects and thus increase our common cyber-resilience.

In particular, we call for:

- greater transparency and responsibility by both States and non-state actors in the handling of vulnerabilities, including their discovery, reporting, and stockpiling;
- further promotion, on a global scale, of clear processes for responsible vulnerability reporting and disclosure.

Fortunately many good practices exist in the cybersecurity industry and CERT/CSIRT community, and there is much helpful guidance provided by some governments. We at Kaspersky follow five ethical principles in responsible vulnerability disclosure[8], and many other mature players follow the same. However, we need greater transparency about that from other less mature organizations as well as from States themselves.

---

[6] https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

[7] Day 0 Event #41 Cyber Stability Games: Learning the Complexities of Technical Attribution https://www.intgovforum.org/en/content/igf-2021-day-0-event-41-cyber-stability-game-learning-the-complexities-of-technical

[8] Kaspersky's ethical principles in Responsible Vulnerability Disclosure https://media.kasperskydaily.com/wp-content/uploads/sites/92/2020/05/15091233/RVD-Ethical-Principles-EN.pdf

kaspersky

5. ***Enhancing interoperability and harmonization of emerging national regulatory practices to secure ICTs as well as to regulate critical infrastructure protection and to ensure the ICT supply chain security and integrity***

We have called in the past and continue calling for developing more concrete tools for critical infrastructure protection, security-by-design in modern ICTs, as well as for ICT supply chain security and integrity. These concrete tools could include the development of good practices guides, baseline security requirements, certification and labelling for ICTs, software transparency (such as a software bill of materials) and others. And as company working globally in different countries and regions, we see the growing development and adoption of similar concrete tools as following initiatives from either governments or industry.

At the same time, the risk of fragmented approaches across States, jurisdictions, and sectors to develop such tools and regulate the security of still globally developed, distributed, and consumed ICTs poses a threat and could potentially lead to greater insecurity. Therefore, enhancing interoperability and harmonization of such emerging national regulatory practices and industry approaches is necessary to both ensure the security of ICTs and to keep them open and accessible across different physical boundaries in cyberspace.

We are proud to discuss these risks within different multistakeholder fora such as the Geneva Dialogue on Responsible Behavior in Cyberspace[9], the OECD work on Digital Security[10], and the Paris Call for Trust and Security in Cyberspace[11], where in the latter we co-chaired Working Group 6 and produced a report[12] on policy gaps in building stronger ICT supply chain security. We would be happy to contribute to discussions on this topic within the UN OEWG and share our experience in this regard.

6. ***Building an institutional framework for an international cyber incident response in case of significant cyber incidents affecting international security and peace***

In the event of a significant cyber incident affecting critical infrastructure either located within one State or several States, it is important to effectively and timely coordinate actions between States as well as relevant CERTs/CSIRTs, owners of the affected critical infrastructure, security providers, software providers and more. And quite often in practice the victim organization starts looking for the right contact to work on incident response and mitigation, and precious time can be lost.

As a party that can be engaged in a global incident response and as a security provider that can support affected organizations with analysis and remediation of a cyberattack, we do still have limited resources and insights into the global threat landscape and capacities. Therefore, we call for greater cooperation among States as well as relevant non-state actors (as mentioned in the para above) to ensure the security and safety of users. Practically speaking, we call for:

[9] https://genevadialogue.ch/
[10] https://www.oecd.org/digital/ieconomy/digital-security/
[11] https://pariscall.international/en
[12] https://pariscall.international/assets/files/2021-11-12-Paris-Call-Working-Group6-Report-SecuringICTSupplyChain.pdf

- 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.

At the same time, for such a global incident response it is vital to enhance coperation between the CERT/CSIRT community and security researchers and avoid creating political and administrative barriers to such cooperation. Despite the political or geopolitical context, this is vital to ensure continuous cooperation between the CERT/CSIRT community and security researchers as essential firemen in protecting users in case of cyber incidents.

This cooperation usually includes the exchange of threat information, cyber incident reports, vulnerability information and others, and therefore it is important to avoid creating political and administrative barriers to such information exchange.

Being a part of the international research project within the UN IGF Best Practice Forum (BPF) on Cybersecurity[13], we have conducted a study investigating how the international community responded to past significant and well-known security incidents, and where those security incidents have triggered norm implementation or further norm development. Having conducted interviews with actual practitioners involved in the mitigation of those security incidents, we learned how critical the free flow of information and cooperation between vulnerability analysts, security researchers and incident responders is, and in many cases the possibility to cooperate across borders plays a defining moment in protecting users.

7. Identifying and protecting, in a global coordinated action, broadly used security and critical open-source tools and libraries that compose the public core of the internet infrastructure

In complementarity with ongoing efforts to define, identify, regulate and ensure the security of critical infrastructure protection which is a prerogative of States, it is important to protect commonly and broadly used security and critical open-source tools and libraries that compose the public core of the global internet infrastructure. The efforts to ensure the availability and security of these should be coordinated, as they are critical for conducting in-depth assessment and vulnerability research.

8. Enhancing transparency about activities in cyberspace to bring greater predictability and stability

In the spirit of the UN OEWG itself and its commitment to transparency and openness, we continue calling for greater transparency about activities in cyberspace. In particular, we believe it is important to enhance transparency about:

[13] Testing Norms Concepts Against Cybersecurity Events, UN IGF BPF on Cybersecurity, December 2021, https://www.intgovforum.org/en/filedepot_download/235/20025

- Member States' activities in cyberspace through publicly informing the rationale behind their decision-making to reduce uncertainty about processes in cyberspace. The publication of States' cyberspace strategies, doctrines and other relevant documents could be particularly useful here;
- ICT capabilities for military purposes to ensure that these capabilities are used in accordance with international law and do not undermine international security or adherence to agreed-upon norms related to responsible behavior in cyberspace. If this is followed, it would in particular help address the threat identified as States themselves in the 2021 UN OEWG report in para 16[14].

Conclusion

The 2021 OEWG report stated that the active engagement of all delegations has demonstrated the determination of States to work together. We would also add that not only States, but an increasingly broad, diverse and large community of non-State actors, including companies, technical experts, academia, and civil society, have demonstrated both their strong interest and a readiness to support the States' efforts to ensure a stable and secure cyberspace. And we look forward to continuing doing so.

About Kaspersky

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 270,000 corporate clients protect what matters to them most. Learn more at www.kaspersky.com.

[14] https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf