AO Kaspersky Lab
39A/2 Leningradskoe Shosse,
Moscow, 125212, Russia

+7 495 797 87 00
www.kaspersky.com
www.securelist.com

Comments on the second 'Pre-draft' of the report of the Open-Ended Working Group ('OEWG') on developments in the field of information and telecommunications in the context of international security

Kaspersky Position Paper

June 2020

Introduction

Kaspersky welcomes the opportunity to provide comments on the second 'Pre-draft' report. We remain grateful that the OEWG, particularly the Chair, Ambassador Jürg Lauber, continues to share relevant documents and to solicit input from various stakeholders as part of its ongoing commitment to inclusivity and transparency, with the aim of maintaining and promoting trust. Kaspersky contends that the exchange of views with representatives from non-governmental organizations, civil society, industry, the technical community, and academia is crucial in leveraging expertise on the important issues related to the OEWG's mandate.

Executive Summary

Kaspersky's feedback on the second 'Pre-draft' focuses on three primary areas:

1. Recommendations to further strengthen multi-stakeholder participation in confidence building measures ('CBMs'), capacity-building, and regular institutional dialogue;
2. Recommendations to develop consensus-based measures and concrete tools for protecting critical infrastructure and enhancing the resilience of ICT supply chains; and
3. Suggestions to clarify terminology to further enhance international cooperation on ICT global governance.

Expanding and strengthening multi-stakeholder participation in confidence-building measures ('CBMs'), capacity-building, and regular institutional dialogue

The second 'Pre-draft' report rightfully notes that, "Measures that build confidence and capacity reinforce adherence to international law, encourage the operationalization of norms, provide opportunities for enhanced cooperation between States, and empower each State to reap the benefits of ICTs for their societies and economies."[1] Multi-stakeholder participation can only enhance such efforts, adding tremendous value in terms of expertise, technical knowledge, resources, and support. Academia, civil society, other non-governmental organizations, industry, the technical community, and other private sector entities can play significant roles in raising awareness, promoting good governance, leveraging existing industry- or sector-led frameworks, and assessing the effects of CBMs and capacity-building initiatives. We note that the second 'Pre-draft' report does not explicitly mention the technical community as a key

[1] Open-Ended Working Group, "Second 'Pre-draft' of the report of the OEWG on developments in the field of information and telecommunications in the context of international security," 27 May 2020, paragraph 15. Link: https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf.

AO Kaspersky Lab
39A/2 Leningradskoe Shosse,
Moscow, 125212, Russia

+7 495 797 87 00
www.kaspersky.com
www.securelist.com

stakeholder group and assert that should be remedied. The technical community can contribute valuable expertise and advice that could help ensure evidence-based discussions and outcomes.

In order to encourage further multi-stakeholder participation in developing and implementing "measures that build confidence and capacity" and harness the benefits that result from such participation, Kaspersky specifically recommends that:

1. The proposed repository of CBMs, to be established as a request of the Secretary-General,[2] be made public so that all stakeholders with interests and responsibilities in facilitating cooperation toward an open, secure, stable, accessible and peaceful ICT environment can contribute to their design and implementation;
2. The OEWG, perhaps an appendix to the final report, solicits input on other fora that can promote CBMs, given the second 'Pre-draft' report's acknowledgement that not all States belong to regional organizations and that not all regional organizations have CBMs in place;[3]
3. The final report include a specific recommendation on the establishment of a multi-stakeholder approach to capacity-building in order to address policy and technical gaps, ensure sustainability, assess program effectiveness, and contend with issues raised by emerging technologies;[4] and
4. The final report specifies that national Points of Contact ('POCs')[5] be encouraged to engage non-governmental stakeholders in order to ensure that CBMs are sufficiently "future proof," technology-neutral, supportive of further innovation and technological development, comprehensive, and balanced.

With regards to the second 'Pre-draft' report's provisions related to regular institutional dialogue, Kaspersky agrees that the establishment of such a dialogue could serve as an important confidence-building measure. We also contend that a format that supports implementation and operationalization of existing commitments while engaging in periodic reviews to consider new measures or refinement of the existing normative framework[6] is a reasonable path forward. Kaspersky also supports the proposal to coordinate exchanges between the proposed regular institutional dialogue and other UN fora to avoid unnecessary duplication, identify potential synergies, and improve coherence.[7]

Kaspersky also supports the inclusion of language in the second 'Pre-draft' report, which supports engagements with other stakeholder groups and non-governmental actors, as well as developing appropriate mechanisms for their interventions in a regular institutional dialogue.[8] Such participation is critical given the various roles that these stakeholders play in the ICT environment.[9] Again, we reiterate the importance of explicitly recommending that academia, civil society, other non-governmental actors, industry, the technical community, and other private

[2] Paragraphs 49 and 74 (c).
[3] Paragraph 51.
[4] Paragraph 59.
[5] Paragraphs 48 and 74 (c).
[6] Paragraph 67.
[7] Paragraph 70.
[8] Paragraph 71.
[9] Paragraph 71.

sector actors be allowed to contribute to these dialogues, as well as the mechanisms that might ensure their participation.[10]

Multi-stakeholder contributions to critical infrastructure protection and ICT supply chain resilience

Kaspersky supports further efforts to implement existing obligations and voluntary commitments in accordance with international law, cyber-norms, and CBMs;[11] in particular, we strongly agree that further operationalization of rules, norms, and principles that contribute to strengthening critical infrastructure protection and ICT supply chain resiliency is imperative. The second 'Pre-draft' report notes that critical infrastructure is "owned, managed or operated by the private sector" in many States and, as a result, "inter-State or public-private cooperation may be necessary to protect its integrity, functioning and availability."[12] It also highlights that "the systemic and transnational risks arising from a lack of ICT security, insufficient coordination between technical and policy capacities at the national level, and the related challenges of inequalities and digital divides"[13] can be addressed via capacity-building. Kaspersky agrees with these statements as well.

However, we reiterate the importance of multi-stakeholder approaches to enhancing the protection of critical infrastructure and the resiliency of ICT supply chains. Our recommendations are as follows:

1. The OEWG should consider the establishment of a forum that seeks to align best practices, lessons learned, certification regimes, and interoperable baseline security requirements with existing industry standards and practices, with the aim to enhance the security of, and confidence in, ICT products and services in a technology-neutral and interoperable manner, to the greatest extent possible;
2. The final report should incorporate language in support of transparent vulnerability management, handling, and mitigation programs by States, and similar programs by non-State actors to ensure greater security of both software and hardware components in ICT supply chains. Vulnerability disclosures by States should not be limited to users, as referenced in the second 'Pre-draft' report,[14] but should also include vendors or developers of the ICT products and services as well;
3. The final report should encourage greater transparency on national supply chain and critical infrastructure protection frameworks to provide clarity and guidance for other actors in cyberspace on incident response, incident notification, and security measures for ICT products, perhaps as part of the proposed global repository of CBMs;
4. The final report should stipulate greater cyber-threat information sharing between public and private actors, including private sector entities and the technical community,

[10] Kaspersky, "Position Paper on Initial 'Pre-draft' of the report of the OEWG on developments in the field of information and telecommunications in the context of international security," submitted 30 March 2020, pages 2-3. Link: https://front.un-arm.org/wp-content/uploads/2020/03/kaspersky-position-paper-on-oewg-first-pre-draft-report.pdf
[11] As agreed in the Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, transmitted 26 June 2015, (A/70/174). Link: https://undocs.org/A/70/174.
[12] Paragraph 23.
[13] Paragraph 54.
[14] Paragraph 42.

regarding cyber-related threats, vulnerabilities, and incidents in ICT supply chains to ensure the security of the entire ICT ecosystem; and

5. The OEWG should consider how best to engage non-State actors to achieve focused and outcome-oriented capacity-building efforts aimed at addressing risks to critical infrastructure and ICT supply chains. Kaspersky supports the view of the United Nations Institute for Disarmament Research ('UNIDIR'), which acknowledges that currently there is a lack of capacity building clearly focused on addressing ICT supply chain-related risks.[15] In response to this need, Kaspersky recently launched its Cyber Capacity Building Program to help organizations develop practical tools and knowledge for proper security assessments of the products they use and thus help enhance the cyber-resilience of their own networks. The program includes dedicated training on product security evaluations, threat modeling, source code/technical reviews, and vulnerability management practices.[16] Perhaps, States and non-State actors can iterate on this type of program together.

Greater clarity for consensus-based discussions

As expressed in our submission on the initial 'Pre-draft' report, Kaspersky acknowledges the challenges to a global consensus on the security and stability of cyberspace due to diverse views that may exist in the international community. Nonetheless, a dialogue – open, transparent, and with opportunities for interventions by non-State actors – plays a crucial role in achieving that consensus. To support this process, it is important to use clear definitions and terms related to the ICT environment. We note a lack of clarity in some parts of the second 'Pre-draft' report, and, as a result, we recommend further terminology clarifications as follows:

1. It is important to pursue a technology-neutral approach to ICT governance, as well as to acknowledge both the positive and negative implications of ICT. To strike a balance with regard to the positive implications of ICTs and innovation, we suggest revising the language that refers to ICTs as "dual-use technologies,"[17] as not all ICTs could be used for malicious purposes or have inherently malicious functionalities. This would align with the statement that, "it is the misuse of technologies, not the technologies themselves"[18] that is the cause of concern. In a similar vein, we also note that the introductory words to Section B, "Existing and Potential Threats," describe mostly negative aspects in the use of ICTs, which could limit the understanding of the positive benefits that ICTs offer for humanity. Therefore, we suggest revising the header to "Protecting ICTs from existing and potential threats;"
2. The second 'Pre-draft' report acknowledges the importance of protecting medical facilities from ICT operations, given the potentially devastating impact on human life and safety.[19] Given the expansion of such attacks on hospitals, research facilities, and health-related non-governmental organizations during the current global health crisis, it

[15] United Nations Institute for Disarmament Research ('UNIDIR'), "Supply Chain Security in the Cyber Age: Sector Trends, Current Threats and Multi-Stakeholder Responses," Link: https://www.unidir.org/publication/supply-chain-security-cyber-age-sector-trends-current-threats-and-multi-stakeholder.
[16] For more information, please see here: https://www.kaspersky.com/capacity-building.
[17] Paragraph 5.
[18] Paragraph 21.
[19] Paragraphs 22 and 42.

may be useful to provide clarity about the scope of "medical facilities" to ensure that all of these entities are protected;

3. The second 'Pre-draft' report provides that States have a responsibility to notify users "when significant vulnerabilities are identified,"[20] but does not specify how "significance" should be quantified or qualified. While defining what constitutes significance may seem overly prescriptive, we maintain that some guidance on this issue is necessary in order to reduce potential ICT risks if States determine that certain vulnerabilities do not meet the threshold of "significance" and subsequently decide not to notify users and vendors;
4. Throughout the report, the terms 'digital' and 'ICT' seem interchangeable. If this is the intent, it would be useful to confirm their synonymity; and
5. The second 'Pre-draft' report uses different language when discussing critical infrastructure and critical information infrastructure in the substantive discussion (Sections B-G) compared to the Conclusions and Recommendations (Section H), particularly in the use of 'transborder,' 'transnational,' and 'supranational' critical infrastructure and critical information infrastructure.[21] Consistency throughout the document would be helpful, as would any necessary definitions to delineate between these terms in order to mitigate any potential confusion.

Conclusion

Kaspersky appreciates the opportunity to share its views on the second 'Pre-draft' report. We hope that these comments contribute to the worthwhile goal of achieving common ground and mutual understanding on the peaceful use of ICTs within the global community in pursuit of international security. Kaspersky continues to support the work of the OEWG and looks forward to further opportunities to participate in the process going forward.

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.

[20] Paragraph 42.
[21] Paragraph 42.