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

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

Comments on Existing and Potential Threats in Cyberspace for the Informal Multi-Stakeholder Virtual Dialogue Series

Kaspersky Submission

November 2020

Introduction

Kaspersky firmly supports the OEWG, its work and commitment to the principles of transparency and inclusivity in strengthening cybersecurity and promoting international cooperation in this field.

In light of the OEWG's stated objectives, Kaspersky welcomes the opportunity to provide comments on existing and potential threats in cyberspace for the upcoming Informal Multi-Stakeholder Virtual Dialogue Series. We believe that multiple stakeholder groups – the technical community, the private sector, academia and civil society – have relevant perspectives and expertise that can substantially contribute to the dialogues at the OEWG and other UN processes with regard to ICT developments in the context of international security. We hope our comments below will be helpful for Member State delegations in their discussions and consensus-building on stability and security in cyberspace.

What cyber/ICT related activities do you assess to be the biggest threats to international peace and security?

The list includes, but is not limited to, the following processes and activities we find as the biggest threats to international peace and security:

1. **Attacks on critical infrastructure, including supply chain attacks.** Attacks in the sectors that serve the critical needs of societies have the gravest impact in terms of (i) security implications (reputational and financial loss as a result of an attack); (ii) safety implications (injury or damage to persons or even deaths as a consequence of an attack); and (iii) lack of confidence and trust (in a particular technology or technology manufacturer, market, economy, policy or government measure, or even the entire government as a result of an attack). At the same time, supply chain attacks remain one of the most difficult to detect and prevent – they are becoming more targeted and sophisticated, while malicious cyber operations affecting critical infrastructure may remain undetected or unreported for long periods.
2. **Lack of global response to critical infrastructure protection.** (i) Lack of both common terminology and concepts on what should be considered as critical infrastructure, 'transnational' or 'trans-border' infrastructure; (ii) lack of a common State approach to the role of non-state actors in critical infrastructure protection (CIP); and (iii) lack of a common approach to CIP implementation and, particularly, lack of guidance on how CIP-related non-binding 2015 UN GGE norms (norms 'f', 'g', and 'h') should be implemented – all these open questions, with a risk of increasing institutional fragmentation in the management and protection of ICT infrastructure, pose a threat to a common ability to protect against

cyber incidents and respond to them in a timely manner, and as a result, it makes ICT infrastructure less reliable and less cyber resilient.

3. **Exploitation of vulnerabilities, including in emerging technologies.** While it is impossible to have technology 100% free of vulnerabilities, it is critical to address them in a timely and coordinated manner. Vulnerabilities remain[1] the initial attack vector for compromising IT networks and for launching further cyber operations. Poorly secured and designed IoT devices with a lack of transparency into their list of components (together with more complex supply chains and growing reliance on external code/components) may undermine the security and integrity of operations in infrastructure (smart industry, smart cities, smart homes). 5G has also attracted a lot of attention and shifted the focus of the IT security community to 5G security due to the emergence of vulnerabilities in the technology.

4. **Targeted ransomware.** During recent years, the Kaspersky Global Research and Analysis Team (GReAT) has been continuously warning about a shift toward targeted ransomware, and predicts that attackers will use more aggressive methods to extort money from their victims. In 2020, hardly a week has gone by without news of an attempt to extort money from large organizations – including recent attacks on a number of US hospitals.[2] Some attackers seem to apply greater pressure by stealing data before encrypting it and threatening to publish it; and in a recent incident, affecting a large psychotherapy practice, the attackers posted patients' sensitive data.[3]

5. **False flag attacks and increased attacks in regions that lie along the trade routes between Asia and Europe**. In 2020, we observed several APT threat actors target countries that had previously drawn less attention. Kaspersky's GReAT researchers witnessed various malware used by Chinese-speaking actors against government targets in Kuwait, Ethiopia, Algeria, Myanmar and the Middle East. We also observed StrongPity deploying a new, improved version of their main implant called StrongPity4. In 2020 we found victims infected with StrongPity4 outside Turkey, located in the Middle East.

6. **Geo-politics driving the development of many APT campaigns.** Geo-politics continues to drive the development of many APT campaigns, as seen in recent months in the activities of cybercriminal groups such as Transparent Tribe, Sidewinder, Origami Elephant and MosaicRegressor, and in the 'naming and shaming' of various threat actors by the NCSC and the US Department of Justice.[4]

7. **Increasing development of military cyber capabilities with insufficient transparency on their development and use**. The growing development of cyber military capabilities by some states (e.g., by the UK as recently announced[5]) is taking place while the international community has not reached yet a consensus over how these capabilities should be applied and how their application should be interpreted by states to avoid the escalation of conflicts in cyberspace. The lack of transparency in the development of these

[1] Kaspersky Incident Response Analyst Report 2020 https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2020/08/06094905/Kaspersky_Incident-Response-Analyst_2020.pdf
[2] https://www.techradar.com/news/ryuk-ransomware-returns-and-takes-multiple-us-hospitals-offline
[3] https://threatpost.com/vastaamo-hackers-blackmailing-therapy-patients/160536/
[4] Kaspersky APT trends report Q3 2020 https://securelist.com/apt-trends-report-q3-2020/99204/
[5] https://www.gov.uk/government/news/national-cyber-force-transforms-countrys-cyber-capabilities-to-protect-uk

kaspersky

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

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

capabilities and their use also raises concerns among the IT security community as a potential factor possible in escalation and further leading to militarization of cyberspace.

With respect to the draft "Existing and Emerging Threats" section of the OEWG the pre-draft report, are there any notable omissions, additions, or statements with which you support or disagree?

Below we share our comments and notes to some paragraphs in the section 'Existing and Potential Threats':

Para	**Comments**
18. '[…] *Concerns were expressed over the development or use of ICT capabilities, as well as stockpiling or non-disclosure of vulnerabilities, for military purposes inconsistent with the objectives of maintaining international stability and security*. […]'	In line with our previous submission,[6] we agree that the development or use of offensive capabilities, as well as stockpiling vulnerabilities, contributes to instability and reduced trust. Further dialogue on stakeholders' perceptions of threats and vulnerabilities, the importance of ensuring the integrity of the ICT supply chain, and the responsibility of states to notify users when significant vulnerabilities are identified are all critical. However, the Pre-draft does not reference any concrete recommendations or proposals on how to engender such discussion and develop accountability mechanisms to address these concerns. In line with a voluntary, non-binding norm on 'responsible reporting of ICT vulnerabilities,' as recommended in the UN GGE Report 2015 (A/70/174), we support both the creation of coordinated vulnerability handling and mitigation processes[7], as well as vulnerability equities processes by Member States (as suggested by the Global Commission on the Stability of Cyberspace[8]), and coordinated vulnerability disclosure programs by non-state actors.
18. '[…] *Concerns were also noted about the exploitation of harmful hidden functions and the integrity of global ICT supply chains.* […]'	In line with the threats outlined to question #1 above, we believe the issue of supply chain security and integrity is crucial for international security. Additional thoughts and proposals to address this issue would be welcome within the report. We also support the development of universal

[6] Comments on the initial 'Pre-draft' of the report of the OEWG on developments in the field of information and telecommunications in the context of international security, March 2020 https://front.un-arm.org/wp-content/uploads/2020/03/kaspersky-position-paper-on-oewg-first-pre-draft-report.pdf

[7] With the development of coordinated vulnerability handling and mitigation processes, state actors can intake vulnerability reports from external researchers with regard to state networks and systems and thus contribute to enhancing the security and resilience of those networks and systems.

[8] https://cyberstability.org/norms/#toggle-id-5

	interoperable and evidence-based criteria for assessing the security, integrity, and trustworthiness of technologies to avoid disruptions to global ICT supply chains.
21. '[…] *States confirmed that measures to promote responsible State behaviour should remain technology-neutral, underscoring that it is the misuse of such technologies, not the technologies themselves, that is of concern*. […]'	We would like to highlight our strong support of this sentence.
22. '[…] *States underscored that attacks on critical infrastructure (CI) and critical information infrastructure (CII) pose a threat not only to security, but also to economic development and livelihoods, and ultimately the safety and wellbeing of individuals.* […]'	In line with this sentence, in para 22 we believe that a common State approach to critical infrastructure protection (CIP) should be developed to ensure international security. Particularly, further guidance on operationalization of the CIP-related non-binding 2015 UN GGE norms[9] would be very helpful. Since there is still a lack of clarity as to what should be considered a 'trans-border', or 'supranational' critical infrastructure, the international community needs cooperative working mechanisms for addressing cyber incidents affecting critical infrastructure, including in multiple countries. Such cooperative mechanisms among States should engage CERTs and, where needed, the private sector – both owners of critical infrastructure and cybersecurity service providers.
23. '[…] *States observed that CI and CII are defined differently in accordance with national prerogatives and priorities.* […]'	Kaspersky acknowledges the challenges to achieving a global consensus on ICTs and international security due to the different views of some Member States regarding terminology and definitions (e.g., cybersecurity versus information security). Nonetheless, it is crucial to continue intergovernmental consultations with interventions by non-governmental actors – including industry, technical experts, the legal community, and academia – toward consensus-based terminology and definitions of critical infrastructure, cyberthreats, cyberattacks, cyberspace, and other terms. In the Pre-draft, there are a number of similar terms referenced, such as 'digital

[9] These norms focus on CIP and instruct states not to conduct or support ICT activity that intentionally damages critical infrastructure (CI) (norm 'f'); to take appropriate measures to protect CI (norm 'g'); and to respond to appropriate requests for assistance by other states whose CI is under cyberattack (norm 'h').

	technologies,' 'digital space,' 'ICT capabilities,' 'ICTs,' and 'ICT environment.' However, the document does not specify whether these terms are interchangeable or synonymous. Therefore, Kaspersky suggests a CBM-related recommendation to further intergovernmental consultations with interventions by non-state actors on developing a common lexicon with consensus-based terminology and definitions related to the use of ICTs.
23. '[…] *In many States such infrastructure is owned, managed or operated by the private sector. In addition, CI and CII may be shared or networked with another State or operated across different States and jurisdictions (sometimes categorized as transborder, transnational or supranational infrastructure). As a result, inter-State or public-private cooperation may be necessary to protect its integrity, functioning and availability.* […]'	Like Member States, Kaspersky also maintains that the protection of national critical infrastructure and supranational critical information infrastructure is paramount. Kaspersky also supports the view of some Member States, communicated via national submissions to the 'Pre-draft' of the UN OEWG report, regarding the necessity to 'increase exchanges on standards and best practices with regard to critical infrastructure protection and encourage enterprises to embark on such exchanges.' These exchanges with private sector entities should endeavour to develop concrete tools – good practices, lessons learned, certification regimes, and interoperable baseline security requirements aligned with existing international standards.[10] Because private sector entities, in particular, own and operate most critical infrastructure, we recommend that language relating to increased exchanges on standards and best practices with regard to critical infrastructure protection with non-governmental organizations, academia, and the private sector be included as a CBM.

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.

[10] As an example of successful efforts – the Geneva Dialogue on responsible behavior in cyberspace, an international conversation led by the Federal Department of Foreign Affairs, Switzerland and DiploFoundation, focused on the security of digital products and services. As a result of consultations with representatives of industry, the Geneva Dialogue published the baseline good practices for reducing vulnerabilities and secure design https://genevadialogue.ch/wp-content/uploads/Geneva-Dialogue-Output-document-for-comments-v20201110.pdf