kaspersky

KASPERSKY'S CONTRIBUTION
TO THE INFORMAL DIALOGUE UNDER THE AEGIS OF THE
OPEN-ENDED WORKING GROUP ON SECURITY OF AND IN THE USE OF ICT
(July 11, 2023)

Mr. Chair,
Excellencies,
Distinguished colleagues,

On behalf of Kaspersky cybersecurity company, let me thank you for the opportunity to participate in this important and timely discussion. Kaspersky welcomes the commitment of the Open-Ended Working Group on the security of and use of information and communication technology (hereinafter referred to as "the OEWG") to engage non-state stakeholders (including businesses, non-governmental organizations and academia) in a systematic, sustained and substantive manner. Taking into consideration the important role that private actors play in designing and utilizing ICT, we believe that their expertise can be valuable contribution to creating favorable conditions for sustainable development and use of ICT.

In my speech, I would like to focus on the issue of supply chain risk management, reflected in Chapter C of the Zero Draft of the Second Annual Progress Report (hereinafter referred to as "the Report"). The extended remarks will be shared later in the written form with the UN Office for Disarmament Affairs.

In providing security for supply chains, it is important to take into account the fact that a vulnerability of a single element poses substantial risks for the whole supply chain as cybercriminals try to find and exploit the weakest link to perform cyberattacks. In this regard, all elements of supply chains, as well as their producers and distributors, should be the subject to a comprehensive assessment aimed at identifying potential risks.

In our view, effective policy in supply chain risk management can be developed and implemented only by working with both suppliers and customers of ICT products and services. On the one hand, governments could consider introducing relevant regulation combined with non-binding guidelines (for example, self-attestation mechanisms) that would establish comprehensive evidence-based certification schemes for ICT vendors. On the other, a framework should be developed that would incentivize customers to prioritize the safety of products and services they procure. We believe that only such a two-pronged approach could greatly contribute to promoting production and use of secure IT solutions in supply chains while simultaneously eliminating loopholes for utilization of vulnerable IT products and services.

At the same time, the corporate sector (for instance, ICT vendors) could also contribute to the creation of an effective supply chain risk management framework. This could be done, in particular, through implementing self-evaluation mechanisms as well as through enhancing transparency for potential customers. To illustrate, Kaspersky, for its part, implements the Global Transparency initiative (GTI) aimed at proving the security and trustworthiness of its solutions to

kaspersky

existing and potential partners through demonstration and verifiable testing[1]. We advocate for other IT vendors to develop and implement similar mechanisms to promote transparency and thus security of the industry overall.

Particular attention should also be paid to the issues connected with the use of open-source code in creating ICT solutions for supply chains. Although it provides ample opportunities for ICT developers worldwide, the utilization of open-source software poses significant risks for supply chains as it has more vulnerabilities and thus is prone to exploitation by malicious actors. In order to counter these threats, collaborative private-public measures need to be developed to enhance the trustworthiness of open-source software. The corporate sector could also positively contribute to securing open source components. In particular, IT leading vendors could invest in developing secure-by-design open source modules that can be used by all industry members including small and medium-sized businesses.

On a global level, Kaspersky firmly supports efforts aimed at strengthening international dialogue on supply chain risk management. In our view, the focus here could be on improving mechanisms for sharing and implementing best practices, including, webinars and other forms of training. In this regard, we also support the idea of establishing a voluntary glossary of key technical ICT terms to promote mutual understanding. At the same time, we believe that the corporate sector could play a greater role in promoting the building of cyber capacity with respect to supply chain risk management, as leading ICT vendors, including Kaspersky itself, already have a wealth of experience in providing training to cyber authorities, other government agencies and businesses around the world, particularly, in developing countries.

In conclusion, Kaspersky reiterates its support for work of the OEWG aimed at fostering international cooperation on countering cyberthreats and creating favorable conditions for the use of ICT worldwide.

I thank you for your attention.

Yours sincerely,

Yuliya Shlychkova

Head of Public Affairs,

Kaspersky

[1] In June, the GTI marked its 5th anniversary. You can find major highlights here