kaspersky

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

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

Contribution to the Paris Call for Trust and Security in Cyberspace Open Consultation – Feb. 26, 2020

1. Foresight

a. In your opinion, which technology may have the most destabilizing impact in the coming months or years? (500 character limit)

(1) Machine learning enabling attacks with the ability to adapt and compromise systems with minimal chance of detection; (2) IoT and interconnected systems embedded into smart cities and smart industries, including critical infrastructure; (3) distributed ledger technologies used by crypto-criminals; (4) quantum computing and the questions it raises about the security of modern cryptography and encryption methods.

b. In your opinion, which technological innovation has the most promising cybersecurity applications? (500 character limit)

The widespread inclusion of IT and cybersecurity in education and training programs from an early age will open up major avenues of research and innovation, while securing us from many of today's common cases of ICT threats. Alternatively, as a more conventional, short-term response, research powered by machine learning is already providing insights for malicious code classification, attack detection, and automated incident response.

c. Have you put in place specific actions in response to these new threats and opportunities? (Yes/No)

Yes.

d. Which actions? (500 character limit)

Our solutions and services provide threat intelligence and highly qualified human expertise. We invest in education, awareness-raising initiatives alongside academia, the tech community and public sector; develop innovations with Horizon 2020 projects. We've also developed a 'cyber-immunity' concept with a secure by design approach - designing IoT, ICS and critical infrastructure with security in mind, allowing deep integration with cybersecurity, making them immune to cyberattacks.

2. Individual rights

a. In your opinion, are citizens' rights sufficiently protected in the face of dangerous practices developing in cyberspace (cybercrime, theft of personal information, information manipulation, electoral interference...)? (Yes, absolutely / Yes, partially / No, insufficiently / Not at all)

No, insufficiently

b. How can they be better protected? (500 character limit)

It's the common responsibility of all of us to protect citizens. That's why we call for greater synergy between actors for global capacity building and the creation of PPPs to secure citizens and increase global cyber-resilience, including through education, research and training. We launched the Global Transparency Initiative to raise user confidence in cybersecurity by increasing the transparency of our products and processes and calling on industry to enhance software development practices.

c. In your opinion, how can we guarantee the application of international human rights law and international humanitarian law to cyberspace? (Select an option: By placing more trust in private actors / By opening discussion on this topic that would involve all relevant stakeholders / By conducting negotiations within international organizations (UN, OECD, EU, Etc.) / By creating tool for imposing sanctions on actors who do not respect these norms)

By opening discussion on this topic that would involve all relevant stakeholders

kaspersky

d. Should providers of digital services and products have a duty of care to protect their users from online risks? (Yes, absolutely / Yes, possibly / Probably not / Absolutely not)

Yes, absolutely

3. Advancing security

a. Do you take any special measures to ensure digital security of your products and services? (Yes / No)

Yes

b. In your opinion, what minimum norms or standards should companies selling digital products and services adhere to? (500 character limit)

Companies should adhere to the 2015 UNGGE norms and GCSC framework: (a) develop and apply security measures, including standards and certifications; (b) exchange threat and incident information with industry and competent authorities; (c) ensure the integrity and security of supply chains; (d) encourage responsible vulnerability disclosure and mitigate significant vulnerabilities. Under GTI, we passed 2 audits to confirm the security of our processes and run the vulnerability management program.

c. In your opinion, what measures could be taken at the national or international level by states to ensure the protection of civil critical infrastructure? (500 character limit)

A holistic strategy includes (1) designated priorities, sector specific CERTs, competent authorities; (2) cooperation between these authorities and industry to develop sector specific guidelines and min security baselines; (3) incident reporting with thresholds according to risk; (4) private-to-public and vice versa threat info sharing; (5) government-industry supply chain security taskforce; (6) national CVD and gov. equities process; (7) consultations for security by design IoT best practices.

d. Do you think these measures should be mandatory? (Yes/No)

N/A (all measures mentioned in the previous answer all not regulatory)

e. What mechanism or procedure do you have at your disposal in the event of a cyber attack or incident on your infrastructures? (500 character limit)

We have an incident management policy approved by Kaspersky's CISO and CEO. It prescribes the necessary measures, including penetration testing and digital forensics for investigation, cooperation between certain teams to develop incident response & mitigation, if necessary. Our policy has been audited by one of the 'Big Four' which confirmed its compliance with the SSAE 18 standard within the SOC 2 reporting framework. Detailed audit https://www.kaspersky.com/about/compliance-soc2

f. Do you have the ability to inform your authorities of a cyber incident that would affect you? (Yes / No)

Yes

4. Capacity building and technical cooperation.

Capacity building refers to supporting the development of cyber defence capabilities of public and private entities through training and coaching programmes, technical assistance, and the exchange of resources and expertise.

a. What are the capacity building needs of your organization or country? (500 character limit)

It is critical that capacity building focuses not just on government stakeholders but industry and civil society as well. At Kaspersky we hope to see greater synergy between states and the private sector to deliver multistakeholder solutions to train and educate individuals, private entities and public authorities.

Awareness and transparency are also critical, as capacity-building efforts can only succeed if they are responding in a targeted way to a real need.

b. Do you have the resources to contribute to capacity building in your community, in your country or in other countries? (Yes / No)

Yes

c. How are you willing to contribute to capacity building? (500 character limit)

Kaspersky contributes to capacity building by (1) providing trainings on malware analysis, incident response etc.; (2) sharing threat intelligence and providing access to Kaspersky's Threat Attribution Engine for malware analysis; (4) offering open source- Bitscout – and freemium tools for law enforcement agencies; (5) sharing expertise on governance aspects through public-private consultations; (6) raising awareness through education initiatives.

d. Which capacity building or international cooperation initiative impressed you the most last year? (500 character limit)

We are proud to be one of the co-founders of the NoMoreRansom initiative – a non-commercial public-private project to help ransomware victims free. As a gold standard in terms of collaboration between law enforcement and the private sector, it units more than 150 multistakeholder partners and has helped more than 200,000 victims of ransomware recover their files free of charge, preventing some $108 million from going into the wrong pockets.

e. What, in your opinion, is your organization's main weakness in terms of cybersecurity? (500 character limit)

N/A

5. Multi-stakeholder cooperation

a. Do you collaborate, on your level, with public authorities, businesses and/or civil society organizations? (Yes / No)

Yes

b. How? (500 character limit)

We support multistakeholder intiatives for a more secure and stable cyberspace, including the French platform 'Cybermalveillance' to secure citizens and SMEs; the Paris Peace Forum which we supported in 2019; Internet Governance Forum. We collaborate with other parties via the expert group on Industry 4.0 at ENISA which we are a member of; Horizon 2020 projects where we cooperate with academia, researchers and the tech community; other industry country-specific dialogues.

c. What obstacles do you think impede cooperation between governments, the private sector and civil society? (500 character limit)

Different motivations of parties prevent quick results, consensus-based solutions. Europe is quite successful in regulations and policies, but implementation remains is not coherent. There is a lack of coordination between intergovernmental normative initiatives, industry, states and the tech community; overlaps in multistakeholder frameworks. Perhaps more harmonized, regular single institutional dialogue under the UN with broad participation including the industry, would improve things.

What do you think is the most appropriate multi-stakeholder forum for discussions on cyberspace? (500 character limit)

We believe that the IGF could unite many stakeholders and address highly diverse and complex issues connected with cybersecurity, internet governance and ensuring that cyberspace remains secure, stable and open.

6. The principles of the Paris Call and the UN process.

Two negotiation processes have begun at the United Nations in 2019 on the security of cyberspace. Established working groups deal with the application of international law to cyberspace, the production of norms for responsible behaviour by states, and the development of confidence-building and capacity-building measures.

a. **Among the 9 principles of the Paris Call, which 3 seem to you the most fundamental for the maintaining of peace and security in cyberspace? (choose 3 of them)**

1, 6 and 9:

1- Protect individuals and infrastructure. Prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure.

2- Protect the Internet. Prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet.

3- Defend electoral processes. Strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities.

4- Defend intellectual property. Prevent ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sector.

5- Non-proliferation. Develop ways to prevent the proliferation of malicious software and practices intended to cause harm.

6- Lifecycle security. Strengthen the security of digital processes, products and services, throughout their lifecycle and supply chain.

7- Cyber hygiene Support efforts to strengthen an advanced cyber hygiene for all actors.

8- No private hack back. Take steps to prevent non-State actors, including the private sector, from hacking-back, for their own purposes or those of other non-State actors.

9- International norms. Promote the widespread acceptance and implementation of international norms of responsible behavior as well as confidence-building measures in cyberspace.

b. **Which of these principles would you like to see addressed at the UN? (Choose as many as you like)**

All of them.

c. **In your opinion, are there other cybersecurity issues that should be dealt with at the UN? (500 character limit)**

We believe it is important to work more on consensus among states and non-state actors over (1) ways to address emerging threats and new technologies; (2) the application of international law, including the application of IHL to cyberspace; (3) regular institutional dialogue; (4) transparency from states over their cyber capacity programs, including military and defense programs.

d. **What level of knowledge do you think you possess about past and ongoing work at the UN on cybersecurity issues? (0 (none) to 4 (very good))**

3

7. About your organization

a. **Name of your organization (This information will not be made public).**

Kaspersky

b. **Contact email (This information will not be made public).**

arnaud.dechoux@kaspersky.com ; Oleg.Abdurashitov@kaspersky.com

c. **Are you a supporter of the Paris Call? (Yes / No)**

Yes

d. **You are (A government / A public or local authority / A company or trade association / A civil society organization)**

A company or trade association

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 most to them. Learn more at www.kaspersky.com.