kaspersky

KASPERSKY'S SUBMISSION TO THE SIXTH SESSION OF THE AD HOC COMMITTEE TO ELABORATE A COMPREHENSIVE INTERNATIONAL CONVENTION ON COUNTERING THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES FOR CRIMINAL PURPOSES

(August 21 – September 1, 2023)

Kaspersky firmly supports the continuous efforts of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (hereinafter referred to as "the Ad Hoc Committee" or "the AHC"), the Committee Chair, and the Secretariat in preparing the Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (hereinafter referred to as "the Convention").

Kaspersky acknowledges the importance of a comprehensive and effective framework with clear guidelines and best practices to cooperate in order to tackle the growing threats posed by cybercrime, while ensuring the protection of human rights and privacy. As a company, we have more than 25 years of global experience in helping fight cybercrime by developing cybersecurity solutions. Protecting businesses and citizens from cyberthreats is the foundation that permits us to speak confidently on this matter.

Kaspersky also appreciates the opportunity provided by the Ad Hoc Committee to members of the multi-stakeholder community to meaningfully engage in the discussions aimed at elaborating the Convention. We believe that participation of non-state stakeholders with vast expertise in the IT domain greatly contributes to the process of developing the Convention.

In this submission paper, Kaspersky aims to contribute to the ongoing negotiating process focusing on the following points reflected in the draft text of the Convention.

General Provisions

Kaspersky firmly supports the purposes of the Convention outlined in Article 1, including strengthening measures to prevent and combat cybercrime while protecting users from such threats, as well as promoting international cooperation and exchange of expertise and best practices.

At the same time, Kaspersky draws particular attention to the fact that the Convention largely **overlooks** the groups of **ethical security researchers** and **ethical hackers**. Despite their substantial contribution to countering cybercrime, and thus building a safe and secure digital space, these professionals usually find themselves **vulnerable to unfair prosecution**, which eventually has a negative impact on cybersecurity as a whole.

kaspersky

In this regard, Kaspersky proposes that the following terms be considered for inclusion in Article 2 of the Convention:

- **"Ethical security researcher"** meaning a security professional, employed by a legal entity, who tests [computer systems] [information and communications technology systems/devices], networks, and applications for vulnerabilities or security weaknesses in order to identify potential threats and improve their overall security.
- **"Ethical hacker"** meaning a security professional authorized by a legal entity to test its [computer systems] [information and communications technology systems/devices], networks, and applications for vulnerabilities or security weaknesses in order to identify potential threats and improve their overall security.

Kaspersky also supports **including** in the Convention (in particular, in Chapter II, which covers criminalization aspects) specific **provisions** aimed at ensuring the **proactive legal protection** of ethical hackers and ethical security researchers, who should be entitled to this protection unless they are engaged in actions that cause damage or violate established domestic legislation.

Criminalization

In line with commentaries on the Convention's General Provisions (see above), Kaspersky would like to draw particular attention to **providing legal protection** for **ethical hackers** and **ethical security researchers** who play a significant role in countering cybercrime. These specialists are engaged in finding and responsibly disclosing vulnerabilities and thus reducing opportunities for cybercriminals.

In this regard, we welcome as a first step Article 10 paragraph 2, which states that the misuse of devices and programs for the purpose of committing an offence, such as for the **authorized testing** or **protection** of [a computer system] [an information and communications technology system/device] **shall not entail** criminal liability.

At the same time, Kaspersky supports inclusion of specific **provisions** in the Convention that would reflect **proof of criminal intent** as an **obligatory prerequisite** for determining actions that could be **subject to the Convention**. These provisions are particularly important for cases which involve ethical hackers testing computer systems through attempts of unauthorized access.

Jurisdiction

Kaspersky believes any international mechanisms for cooperation in cybercrime investigations under the future Convention should clearly **define** whose **jurisdiction**

kaspersky

should apply in cases involving private sector stakeholders and other parties that may be involved in such investigations.

Procedural Measures and Law Enforcement

Kaspersky's stance is that the private sector can play an important role in assisting states to keep abreast of the IT evolution, as well as supporting law enforcement agencies in the prevention and combating of cybercrime. First of all, this can be done through sharing expertise, as leading IT companies (including cybersecurity vendors) have acquired vast experience in addressing challenges in the cyber domain. In particular, Kaspersky has a long record of assisting national and international law enforcement agencies in combating cybercrime. Most notably, we work closely with **INTERPOL**, both as an active participant of **Project Gateway**[1], and on a bilateral basis by **sharing** necessary **technical information** and threat intelligence with INTERPOL as well as providing **capacity-building**.

With its vast expertise in combating cybercrime, the private sector (in particular, cybersecurity vendors) can provide law enforcement agencies and courts with **forensic expertise** that can help solve alleged cybercrimes. However, the **procedure** currently in place to organize the acceptance of private forensic expert analysis in court at the request of law enforcement agencies is **ineffective**. In this regard, we propose to consider **including** in the Convention specific **provisions** that would **streamline** the **procedure** of **requesting forensic** expertise for **judicial proceedings**, delivered by IT companies at the request of law enforcement agencies.

Kaspersky's position is that high volatility of electronic evidence determines the need for introducing mechanisms of expedited preservation and seizure of evidence upon request from competent authorities. In this regard, we welcome provisions of Articles 25-26 which would establish processes of **expedited preservation** of **stored data**, as well as **expedited preservation** and **partial disclosure** of **traffic data.**

Kaspersky supports provisions on the **conditions and safeguards** mentioned in Article 24, including **judicial or other independent review**, grounds justifying, and limitation of the scope and duration of a power or procedure. We also welcome multiple provisions of Chapter IV, which provide **confidentiality** of the **expedited preservation of stored computer data** (Article 25) and the **interception of content data** (Article 30), as such measures would enhance the effectiveness of investigations.

Kaspersky also believes that the Convention should place a **greater emphasis on the protection of personal data**. It is clear that law enforcement agencies in their fight

[1] International initiative aimed at fostering data sharing on cyberthreats between private-sector companies and INTERPOL.

kaspersky

against cybercriminals seek greater access to electronic evidence, including user data. However, such an approach presents growing risks for the privacy of personal data.

In this regard, we would like to highlight the following major points, which would be relevant to the provisions of the Convention and provide a solid basis for **well-balanced practices** in **accessing data** by **law enforcement agencies**:

- **Real-time access to traffic data** poses a **significant risk** to the privacy and security of users and, therefore, law enforcement agencies must be **strictly limited** in their ability to obtain such data, to the extent governed by conditions and procedures provided for in applicable treaties of States Parties and domestic laws regarding criminal offences;
- Provisions should be included in the future Convention detailing **greater transparency and accountability** on behalf of **governments** regarding the data they **request** from private organizations, the crimes that are being investigated, and the purpose of such data requests. **Private organizations** must also be **transparent** with their users, and clauses that promote transparency and accountability should be applicable to private stakeholders as well;
- In cases where sensitive information, such as **biometric data**, is requested, an **additional court order** should be a requirement before service providers can process such requests. Provisions like these would help promote **accountability** and provide **additional safeguards** to users' interests and rights.

International Cooperation

Kaspersky supports the goal of fostering international cooperation, which is set out in the Convention. We also welcome provisions aimed at accelerating mutual assistance procedures. Time is usually critical in investigating cybercrimes, so the need for streamlined procedures is urgent. We welcome in particular paragraph 12(b) of Article 40, which highlights ensuring the prompt and proper execution or transmission of requests, as well as Article 41, which designates points of contact within the global 24/7 global network, and Articles 42-43, which introduce standards for international cooperation on expedited preservation of stored data and expedited disclosure of preserved traffic data, respectively.

At the same time, Kaspersky draws particular attention to the fact that all such procedures must be in strict compliance with principles ensuring the protection of personal information. In this regard, we welcome the inclusion of these provisions in Article 36, which stresses the protection of personal data obtained by States Parties through international cooperation processes.

kaspersky

In line with its proposals for Chapter IV (Procedural measures and law enforcement), Kaspersky also suggests that consideration be given to including specific provisions to streamline the procedure of requesting and using forensic expertise, provided by an IT company from one State Party, for judicial proceedings in another State Party. Such a measure would be particularly useful in investigating and prosecuting cross-border cybercrimes, especially those affecting developing countries.

Preventive Measures

Kaspersky supports the general provisions on preventive measures outlined in Article 53. In particular, we welcome the intention to **strengthen cooperation** between **law enforcement agencies** and other **relevant entities**, including the **technology sector.**

At the same time, our stance is that Convention could better reflect specific measures aimed at preventing cybercrime as a proactive approach is essential in improving the fight against cybercriminals. In particular, one could consider using the concept of a 24/7 network to expedite the exchange of information between States Parties which could be used for cybercrime prevention.

Kaspersky also **supports** the plans, highlighted previously in the *Consolidated negotiating document on the preamble, the provisions on international cooperation, preventive measures, technical assistance and the mechanism of implementation and the final provisions of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes*, to create a **multilateral repository**, administered by the UN Office of Drugs and Crime, enabling the **dissemination of best practices** in combating cybercrime. Kaspersky has vast experience in sharing its best practices with all interested parties and would be **ready** in principle to **contribute** to creating this repository.

Technical Assistance

Kaspersky supports the general principles of technical assistance and capacity-building, which are outlined in Article 54 the Convention.

At the same time, Kaspersky believes that the Convention **could better reflect** the contribution of the **private sector** for enhancing cyber capacity-building and technical assistance. In particular, leading IT companies, including Kaspersky itself, are already widely engaged in sharing expertise and best practices in cybersecurity with government bodies with a particular focus on developing countries, as well as creating and providing training courses for specialists worldwide.

In this regard, Kaspersky proposes that the Convention should consider **including specific provisions** that would **encourage States Parties** to establish and expand

kaspersky

public-private partnerships in the sphere of **cyber capacity-building**. To date, the importance of public-private cooperation in cyber capacity-building is just briefly mentioned in Article 54 paragraph 4 and Article 55 paragraph 1 of the Convention. For example, leading **IT vendors** have accumulated **greater experience** in some areas (like analyzing specific cyberthreats), than most **national law enforcement agencies**, and could **share** their **expertise** with public authorities through special **training programs**.

Kaspersky draws particular attention to Article 55 paragraph 2 of the Convention, which de facto **overlooks** the **private sector** as a potential **partner** in **developing** common **definitions**, **standards** and **methodologies**, including best practices to prevent and combat such offences. In this regard, we propose to consider including specific **provisions** that would **secure the role** of **private sector organizations** as important **partners** in **elaborating** standards and best practices to prevent and combat cybercrime.

Mechanism of Implementation

Taking into account a significant role of non-governmental actors in providing cybersecurity, Kaspersky **proposes** to consider **establishing** a **permanent advisory panel** to the **Conference of the States Parties to the Convention** (Article 57). The new consultative could include **experts** from relevant organizations, which have been approved to participate in the Ad Hoc Committee, as well as from other non-governmental entities that may express interest in joining the panel.

In conclusion, the Convention could be a crucial instrument for addressing cybercrime, but it is important to ensure that it neither impedes the work of cybersecurity specialists – including ethical hackers and ethical security researchers who do not violate established domestic legislation – nor creates risks for the safety and security of personal data. With these provisions taken into consideration, the Convention could provide an effective framework for countering cybercrime.

About Kaspersky

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly being transformed 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 220,000 corporate clients protect what matters to them most. Learn more at www.kaspersky.com.

kaspersky

For further information regarding this paper, please reach out to Yuliya Shlychkova (Yuliya.Shlychkova@kaspersky.com), Head of Public Affairs, Igor Kumagin (Igor.Kumagin@kaspersky.com), Senior Project Manager, and Andrey Ochepovsky (Andrey.Ochepovsky@kaspersky.com), Public Affairs Manager.