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

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

Comments Submitted to the Cybercrime Convention Committee (T-CY) of the Council of Europe

Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime

December 2020

Kaspersky is grateful to the Cybercrime Convention Committee (T-CY) for the opportunity to provide comments to the provisional text of provisions for the preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime (further – 'Convention').

We would also like to express our support to the important efforts the T-CY undertakes for providing an international legislative framework for combatting cybercrime. We believe that international trans-border cooperation, including among public and private sectors, is critical for addressing the borderless threats we face in cyberspace. At the same time, since most of the enhanced ways of this cooperation will rely on the exchange of data, including personal data, it is essential that the future Additional Protocol will provide for appropriate data protection safeguards, not only from a fundamental rights perspective, but also to ensure legal certainty, mutual trust and the effectiveness of operational law enforcement cooperation.

Below we provide our comments to certain parts of the provisional text. To discuss the contents of the comments or request additional information, please contact Anastasiya Kazakova, Public Affairs Manager at Kaspersky (anastasiya.kazakova@kaspersky.com).

1. Video conferencing

- Article 2.1. describes cases where a requesting Party may request video conferencing and adds that 'whether one or both Parties shall provide interpretation and transcription services'. We would like to draw attention to possible additional resources and costs that this Article may require from both Parties involved and, therefore, this could be a challenge to the timely and effective implementation of the Article.
- Article 2.2. states that 'where appropriate the request Party may, to the extent possible under its law, take the necessary measures to compel a witness or expert to appear in the request Party at a set time and location'; however, Article 2.2. does not provide details on what those 'necessary measures' can include, or under which law they would be determined.
- For implementing Article 2.4., we would recommend to clarify on whom can be qualified and asked as a 'witness' or 'expert'.
- We would also advise to clarify on who will bear the costs mentioned in three excepting cases in Article 2.5. (a) for the timely and effective implementation of a request for video conferencing.

kaspersky

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

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

2. Joint investigation teams and join investigations

- Article 3.3. notes that the competent and participating authorities shall communicate directly, except that 'Parties may agree on other appropriate channels of communication where exceptional circumstances require more central coordination'; however it remains unclear what 'more central coordination' implies and may entail. We would advise to clarify this part as well as the technical side on how requests are to be exchanged (through which platform and which method would be used for that).
- Article 3.5. in point (c) provides that the Parties may use the information or evidence provided for them to 'prevent a situation in which there is a significant and imminent threat involving the life or safety of a natural person'. As these cases might be interpreted differently across countries (Parties), we would advise to have them specified with certain provisions in domestic legislation to provide necessary clarity on particular situations when the request needs to be implemented.

3. Direct disclosure of subscriber information

- To ensure balanced implementation of requests for direct disclosure of subscriber information, we would recommend to consider the following aspects in regard to the Article 4.3.:
    i. Provisions allowing services providers to consult with authorities prior to implementation of requests, as well as to challenge/object to a request if implementation does not seem feasible, as explained by the service provider;
    ii. Provisions with clarifications on how the obtained information would be used, whether sufficient safeguards would be applied for its use and processing, and whether and under which conditions it would be deleted in line with a purpose limitation principle (Article 5.4 (b) of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[1]) ;
    iii. Provisions enabling independent oversight of the issuing authority that makes requests to ensure lawfulness and transparency in the use of information and data obtained.
- Comparing this part to part 5 'Giving effect to orders from another Party for expedited production of data', we note that the overall legislative framework for requesting direct disclosure of subscriber information does not seem fully clear and, therefore, we would advise to clarify this further for effective implementation. Particularly, we would recommend to clarify how requests are meant to be implemented: should requests and information-seeking be among Parties/Countries (where Parties reach the service providers for assistance), or should requests be sent directly to the service providers without notifying the Country/Party where the service provider is established? How much time is considered as an optimal timing for processing and responding to the request? How much time is given to the service providers to evaluate the request for the direct disclosure of subscriber information?

[1] https://rm.coe.int/16808ade9d

In addition, in some cases the affected person's country of residence might be different from both requested Party (i.e. the country and competent authorities where the service provider is established) and requesting Party (i.e. the country and competent authorities which makes the request). Under these provisions, the competent authorities of the affected person's country of residence, as well as competent authorities of the requested Party (where the service provider is established), seem nor consulted neither required to validate requests. The State of the affected person would therefore be unable to refuse and block inaccurate or unlawful foreign data requests, and this may pose a threat to the person's fundamental and procedural rights as well as to special protection of journalists, doctors, etc. The affected person would not be able to access justice and challenge the data request.

Therefore, we would advise to clarify the framework and consider the involvement of the executing State (i.e. requested Party) and 'affected State' (i.e. the country of residence of the affected person).

4. Expedited disclosure of stored computer data in an emergency

- To ensure balanced implementation of requests for expedited disclosure of stored computer data in an emergency, we would recommend to consider the following aspects in regard to Article 7.3.:

    i. Provisions allowing services providers to consult with authorities prior to implementation of requests, as well as to challenge/object to a request if the implementation does not seem feasible, as explained by the service provider;

    ii. Provisions complementing para (f) on a detailed description of the data sought to clarify, as well how the data obtained would be used to ensure that sufficient data protection safeguards are applied, and whether and under which conditions the data would be deleted in line with a purpose limitation principle (Article 5.4 (b) of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[2]).

5. Emergency mutual assistance

- Article 8.1. states that an emergency means a 'situation in which there is a significant and imminent risk to the life or safety of any natural person'. In case there is the imminent risk as a result of the cyber incident or attack at ICT infrastructure where the private sector entity is the owner of it, it would be important to have a clear legislative framework in place for timely cooperation between relevant authorities and this private sector entity/ICT infrastructure owner. However, the draft text does not provide details on how this cooperation should be organized in the event of emergency, and we would recommend to clarify this.

- Article 8.5. provides that the 'requested Party shall respond to the request on the most rapidly expedited basis possible'. Though we understand that implementing this Article may require many resources which are not evenly distributed among Parties, still it would be helpful to provide reasonable timeframes within this Article

[2] https://rm.coe.int/16808ade9d

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

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

to manage expectations on both sides (requesting and requested Parties) for the timely response.

6. Final thoughts

- We understand that the Convention is tasked to provide the key priorities for the international cross-border work in fighting cybercrime, where the implementation would be provided at the national level by the Parties. To avoid the fragmentation in the implementation of the Protocol's provisions, we would recommend to design a consultative mechanism for the Parties to keep the Secretary General and each other about the progress of the national implementation (particularly clarifications of the provisions in the draft text) and, where necessary, to engage with the industry and technical community to ensure the best practice implementation.