Invitation Article

Challenges Related to Fight Against Cybercrime. A Need to Strengthen International Cooperation

*Markko Künnapu**
Legal Adviser
Criminal Policy Department
Ministry of Justice of Estonia

Abstract

The objective of this article is to highlight the need for additional tools and frameworks for international cooperation. As the cyber threat landscape has considerably worsened in the last few years, in particular during the COVID-19 pandemic, law enforcement authorities worldwide need to take necessary measures to respond to this situation. As there are also new types of crime and modus operandi emerging, countries need to assess their legislative and organizational frameworks, and improve their capacities to detect and investigate these criminal offences. As most of the cases are of cross-border nature and electronic evidence needed for the investigations is stored in other countries, there is a greater dependence on international cooperation in conducting successful investigations. As traditional Mutual Legal Assistance measures don't provide the necessary speed and effectiveness needed to adequately address the cybercrime threat, additional tools need to be developed. So far the Convention on Cybercrime or Budapest Convention has been the only international legally binding treaty on cybercrime and electronic evidence. In order to provide additional measures to supplement the ones established in the Convention, officials have opened discussions about creating the Second Additional Protocol. Although the background work and preparations for the Protocol were conducted over the course of several years, the Protocol negotiations started officially in September 2017. In May 2021 the Cybercrime Convention Committee agreed on the conditions of the Protocol. The Protocol would complement the Convention and provide several new tools and measures for law enforcement authorities. These measures include inter alia Mutual Legal Assistance and disclosure of computer data in emergency situations as well as providing avenues for direct cooperation with Multinational Service Providers. The Protocol will be opened for signature in 2022 and hopefully implementing the measures listed in the Protocol will aid in the fight against cybercrime and increase the effectiveness of international cooperation. As the threats and risks related to cybercrime have increased over the years, it is also time for law enforcement to display a stronger response to this pressing issue.

Keywords

cybercrime, Budapest Convention, international cooperation, COVID-19

* Direct correspondence to Markko Künnapu, J.D; Markko.Kynnapu@just.ee
* This paper originally written by Mr. Markko Künnapu was presented at the keynote session of the Korean Institute of Criminology International Forum 2020 in Seoul, Korea
* http://dx.doi.org/10.36889/IJCJ.2021.007
* Received 22 October 2021; Revised 25 October 2021; Accepted 4 November 2021
INTERNATIONAL JOURNAL OF CRIMINAL JUSTICE, Vol. 3 Issue 2, December 2021, 36-42

BACKGROUND

Governments as well as international organizations are reporting increased numbers related to cybercrime and other cyber-related threats. The current COVID-19 pandemic has brought about additional challenges for law enforcement authorities worldwide. Working from distance online and use of remote tools has increased peoples' vulnerabilities to being victims of cybercrime. Furthermore, lack of awareness about the threats and lack of sufficient preventative measures can facilitate cybercrime. Individuals, businesses and governments suffer more and more from different types of cybercrime.

Cybercrime has also changed in regards to its targets and potential negative impacts, in relation to the nature of its threats to national security, the economy, and political systems. This in turn requires an effective response from governments who need to take measures to prevent, detect and investigate cybercrime.

The current COVID-19 pandemic has already shown that cybercrime has the potential to become even worse, more aggressive, more complicated and more expensive to handle than its previous forms. We have also witnessed more attacks against governments and critical infrastructure, including against the health sector. This also means that the approaches and policies to tackle cybercrime must change accordingly to meet these new threats and trends.

Restrictions, limitations related to physical presence and meetings, and working remotely online have also brought about new threats and vulnerabilities in relation to cybercrime. These factors also have a negative impact on the operation of law enforcement authorities and judiciaries.

Problems related to creating measures to fight against cybercrime have arisen previously. However, the current situation and the complications related to the COVID-19 pandemic amplifies the gravity of these difficulties. This means that both businesses and individuals have increased expectations that governments will ensure safe and secure cyberspace and display effective responses to cybercrime. However, several different indicators reveal that only a small fraction of cybercrime offences are being reported and investigated.

CHALLENGES

There is a need for an effective joint response to cybercrime. Still in many countries legislative framework can be fragmented and capacities to detect and investigate cybercrime are low.

This needs to change and governments have different options to respond. First there needs to be strategic approaches and policies on how to improve capacities for the perpetuation and sustainability of proposed solutions. This includes strategies on cybersecurity and cybercrime, as well as necessary supporting legislative framework.

In regards to the criminal justice response to cybercrime, it is important to highlight substantive and procedural law as well as securing a legal basis for national and international cooperation.

There has to be sufficient capacity and competent and specialized institutions to investigate cybercrime and analyse electronic evidence, including digital forensics. Competent authorities need to have all the necessary resources to perform their duties. Law enforcement authorities and judicial authorities need to pay attention also to training. As technology is evolving and so do threats, it is of utmost importance to provide up to date training for all.

Cooperation has continued to be and will remain a key issue in tackling cybercrime. Most of the data or electronic evidence is currently being stored by private sector entities. There is a need for a legislative framework which would enable swift and smooth cooperation between the public and private sectors. Building trust and a culture of cooperation is relevant, because both sides have a respective role to play in fighting cybercrime. Law enforcement authorities should also consider officially signing cooperation agreements or memorandums of understanding in order to make public-private partnerships fully effective.

Most of the cybercrime offences and cyber-related threats are of cross-border nature. This means that legislative and organizational frameworks are not always sufficient if the sole focus is put on national level cooperation and reliance on domestic competent authorities.

Countries need to learn how to cooperate with each other in the most effective manner. However, this is the area that needs most attention in terms of effectively dealing with issues related to cybercrime. This requires a legal basis for cooperation, ensuring maximum availability of channels for cooperation, and achieving a mutual

agreement between parties about minimum standards. Without securing these conditions, cooperation would not work or would not be effective.

As most of the threats and incidents are of cross-border nature, governments cannot fight cybercrime alone. Even if a country adopts sufficient substantive and procedural law provisions, criminalizes cybercrime and provides necessary tools for law enforcement authorities, there is still an urgent need for international cooperation.

As cybercrime has become a cross-border phenomenon, victims, perpetrators as well as computer systems used may be located in different jurisdictions. This applies also to computer data or electronic evidence needed to investigate the case and identify the perpetrators.

This is often problematic, because countries have different views not only in regards to substantive law (what should be considered as cybercrime), but also often express differing opinions about how international cooperation should operate.

THE BUDAPEST CONVENTION

Every country needs to think about and analyze possible options in relation to this issue and how to improve both legislative frameworks and international cooperation.

Currently, there is only one international legally binding instrument on cybercrime and electronic evidence – the Convention on Cybercrime, also known as the Budapest Convention (The Budapest Convention on Cybercrime, 2001).

The Budapest Convention can serve as a model here, providing not only minimum standards on substantive and procedural law, but also a legal basis for cooperation. It is important to note that the provisions of the Convention can also address other criminal offences where electronic evidence is involved. The Convention uses language that is technology-neutral and can be applied to different types on cybercrimes.

The Convention can be considered an instrument on cybercrime and electronic evidence that has a global impact. Many countries have already joined the Convention, and even more have used it as a guide to develop or update domestic legislation, including substantive and procedural law.

The Convention is also being used on a daily basis for international cooperation and to exchange information. The Convention can be used to request preservation, production and real-time access of data from another party. In addition to mutual legal

assistance and cooperation between central authorities, it provides avenues for international cooperation through its 24/7 network and points of contact.`

2ND ADDITIONAL PROTOCOL

However, there is still room for improvement in order to ensure effective and timely access to electronic evidence that is being stored abroad, including "in the cloud."

When speaking about electronic evidence, one has to think about its particular characteristics, in particular its volatile nature. Computer data can be copied, moved or deleted very fast and this may involve computer systems in multiple jurisdictions. It is often the case that the exact location of data remains unknown, in particular when law enforcement authorities face so-called darkweb investigations.

The prevalent issues that arise here are how to ensure timely access to data, how to secure it and how to obtain it. The Budapest Convention contains several procedural measures related to preservation, production and real-time access to data. However, as data moves fast across the borders, these measures alone might not be sufficient.

There are no boundaries for individuals in cyberspace and they can copy, move, and delete data as they wish, in particular when it comes to different cloud computing services. For law enforcement these boundaries still exist and rules and principles on international cooperation apply.

As existing or traditional mutual legal assistance frameworks were not designed to address electronic evidence and don't provide necessary speed and effectiveness, additional tools need to be developed.

Consultations related to the Second Additional Protocol to the Budapest Convention have been ongoing for years. In September 2017 the Cybercrime Convention Committee started to draft and negotiate the text of the protocol. The main aim is to provide new measures and tools to obtain electronic evidence in addition to traditional mutual legal assistance. These tools would complement existing measures and would cover inter alia direct cooperation with multinational service providers, allowing for faster procedures in emergency situations.

In May 2021 the Cybercrime Convention Committee finally agreed to the text of the Additional Protocol. Although there are still internal consultations taking place at

the Council of Europe level it is expected that it will be adopted by the end of 2021 and opened for signature at the beginning of 2022. The Additional Protocol would be open for ratification for all State Parties to the Convention. This also means that in order to ratify the Protocol, a country needs to first become a party of the Convention (T-CY Protocol Drafting Group, 2021).In regards to the content of the Additional Protocol, it would provide for the following additional tools for law enforcement authorities.

First, it would provide a framework and new measures related to direct cooperation with service providers. These measures address both subscriber data and traffic data, which can be used instead of already available international cooperation measures. As practice has shown, law enforcement authorities request the most subscriber information and traffic data, so it is expected that cooperation would become faster and more effective by implementing this measure.

Special attention has also been paid to requests for domain name registration information and providers who offer domain name registration services. This would also enable enhanced cooperation and allow for easier and more efficient identification of registrants of a particular domain name.

Time and the need for fast responsiveness has always been a challenge for cross-border investigations, in particular in cases where electronic evidence is involved. Therefore, this protocol to establish new frameworks, measures and concrete deadlines for cooperation is unquestionably a huge step forward.

As we have already explained, mutual legal assistance frameworks and measures were not designed to address electronic evidence. Due to its volatile nature, electronic evidence requires a different approach and needs to be dealt with in a faster, more efficient manner.

For this particular reason the protocol also addresses mutual legal assistance and provides additional frameworks and legal bases for emergency situations. These measures include expedited disclosure of stored computer data, including content data as well as emergency mutual assistance.

Still, we need to bear in mind that countries and their legal systems are different. For this reason, the protocol would also provide flexibility. By allowing reservations and declarations, the protocol should satisfy the needs of all countries, in particular those countries who wish to have stronger conditions and safeguards in place. Therefore, certain differences concerning cooperation with individual countries could

remain.

Lastly, the protocol provides for rules that can be also found in other international instruments. These include rules on language that could be used for requests, potential for application of video conferencing, and use of joint investigation teams.

As in the Convention, the protocol pays much attention to conditions and safeguards, including safeguards related to personal data protection. We hope that the new protocol with its additional tools related to electronic evidence will make the fight against cybercrime more effective.

Information about the Convention as well as negotiations and public consultations on the 2nd Additional Protocol is publicly available for viewing at the Council of Europe's Cybercrime Convention Committee website (Cybercrime Convention Committee, 2021).

We hope that the protocol and the result of the years of work towards handling cybercrime will provide suitable measures for all parties involved, as well as necessary added value to the fight against cybercrime. As it is expected that the protocol will opened for signature at the beginning of 2022, this development can also be considered an important milestone at the international level. For example, as the European Union is still negotiating its electronic evidence proposal and United Nations is about to start work on a new instrument, it is crucial to have the text of the protocol already prepared and available for immediate use. Countries can use the protocol as guidance to adapt their legislative and organizational frameworks in order to have more effective responses to cybercrime worldwide.

References

Cybercrime Convention Committee. (2021). Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (Draft). Retrieved from "https://rm.coe.int/0900001680a42c4b"

T-CY Protocol Drafting Group. (2021). Protocol negotiations. Retrieved from "https://www.coe.int/en/web/cybercrime/t-cy-drafting-group"

The Budapest Convention on Cybercrime. (2001). T.I.A.S 131, E.T.S. No. 185. Retrieved from "https://www.coe.int/en/web/cybercrime/the-budapest-convention." Accessed 8 November 2021