Crime in the Digital Age:
Enhancing Capacities of Criminal Justice Institutions across the OSCE Area

24 May 2019, Vienna
Großer Vortragssaal, The Federal Ministry of the Interior of the Republic of Austria

Concept Note

Background

Cybercrime is constantly increasing in scope and sophistication. The growing number of the Internet users worldwide and anonymity of the cyberspace provide more and more opportunities to exploit digital technologies for criminal ends, leading to increased numbers of victims and economic damage. According to a report from February 2018, worldwide costs of cybercrime are estimated at $600 billion per year, i.e. 0.8 % of global GDP.[1]

Thanks to the combination of high profits and relatively low risks, cybercrime has evolved into a consolidated, well-run and efficient business model. "Cybercrime-as-service industry", offering an entire portfolio of "professional services" to anybody who can afford it, has marked considerable growth over the recent years; so has criminal abuse of cryptocurrencies, illicit trade through online market places on the Darknet, production of online child sexual exploitation material, social engineering, card-not-present fraud or financially-motivated malware attacks. There are also new trends such as cryptojacking.[2] In addition to these often complex and sophisticated cybercrime cases, digital technologies and electronic evidence play increasingly important role in "traditional" crime as well. Continuous digitalization of our economies can be only expected to further accelerate all these trends in the future.

With the growing number of criminal activities either facilitated or conducted online, strengthening capacities to address cybercrime and cyber-enabled crime is becoming a priority for criminal justice institutions across the OSCE area. However, investigating and prosecuting this type of crime poses significant challenges for many countries due to the lack of suitable legislative framework, sufficient technical capacities or adequate skills and knowledge on behalf of various criminal justice practitioners. As a result, more and more countries request assistance from international organizations in enhancing their capacities. The Organization for Security and Co-operation in Europe (OSCE), together with other multilateral actors such as the Council of Europe, EUROPOL, Interpol or the United Nations

[1] See *"Economic Impact of Cybercrime – No Slowing Down"* (https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html).
[2] For instance, see annually published *Internet Organized Crime Threat Assessment* by EUROPOL (https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment).

Office on Drugs and Crime (UNODC), is thus becoming more and more active in this field. Given the enormous needs of many countries across the world, no international organization can deal with this challenge on its own.

The OSCE Strategic Framework for Police-Related Activities from July 2012 tasks the OSCE to *"facilitate, at the regional and national levels, capacity-building and the exchange of information and best practices in investigating cybercrime and dealing with cyber evidence […]"*. Since then, the OSCE Secretariat's Transnational Threats Department/Strategic Police Matters Unit (TNTD/SPMU) has been providing capacity-building support to the participating States in this area, moving gradually from ad-hoc training activities in the past to more systematic and long-term approach today. In the summer 2017, TNTD/SPMU launched a two-year regional extra-budgetary pilot project "Capacity Building for Criminal Justice Practitioners Combating Cybercrime and Cyber-enabled Crime in South-Eastern Europe". TNTD/SPMU is also expanding its cybercrime-related activities in Central Asia and South Caucasus. With the project in South-Eastern Europe coming to an end in the summer 2019, it is a good opportunity to take stock of its implementation and discuss the OSCE's role and future activities in this increasingly important area.

Objective and expected outcomes

This event aims to contribute to a discussion on how to address the growing threat posed by cybercrime and cyber-enabled crime to public safety and the rule of law in the OSCE area. In particular, the conference will:

- Take stock of the implementation of the project "Capacity Building for Criminal Justice Practitioners Combating Cybercrime and Cyber-enabled Crime in South-Eastern Europe" (2017-2019) and identify key lessons learned, good practices and remaining gaps;
- Discuss priority areas for the OSCE's future work in the field of combating cybercrime and cyber-enabled crime in South-Eastern Europe as well as other sub-regions of the OSCE, namely Central Asia, Eastern Europe and South Caucasus;
- Explore key elements of effective capacity-building assistance by multilateral organizations such as the OSCE to national criminal justice institutions in combating cybercrime and cyber-enabled crime.

A conference report summarizing key findings and outcomes will be published after the event.

Format

The conference is organized by TNTD/SPMU in close co-operation with the Slovak OSCE Chairmanship and support of the Federal Ministry of the Interior of the Republic of Austria.[3] The event will be held in English only and is open to all members of the OSCE Delegations

[3] This activity is financed through the extra-budgetary project No. 1101901 "Capacity Building for Criminal Justice Practitioners Combating Cybercrime and Cyber-enabled Crime in South-Eastern Europe". Donors to this project include Germany, United States of America, Italy and Slovakia.

as well as criminal justice practitioners and relevant experts from the OSCE participating States and Partners for Co-operation.

The event will consist of four sessions. The first session will set the scene by discussing the main features that make cybercrime and cyber-enabled crime an increasingly potent threat to public safety and the rule of law as well as the key challenges faced by criminal justice institutions in this regard. It will also explore how criminal justice system should best respond to this phenomenon and how multilateral organizations such as the OSCE can support these efforts.

The second session will focus on key elements of effective capacity building in combating cybercrime and cyber-enabled crime. It will also discuss most common challenges when implementing capacity-building projects in this area and how to ensure their long-term sustainability and local ownership.

The next session will review the implementation of the project "Capacity Building for Criminal Justice Practitioners Combating Cybercrime and Cyber-enabled Crime in South-Eastern Europe". It will present key outcomes and achievements as well as main challenges encountered during the project's implementation. It will aim to identify key lessons learned from this pilot initiative for other similar capacity-building projects of the OSCE in the future.

The final session will be devoted to future OSCE activities in combating cybercrime and cyber-enabled crime. It will discuss what thematic areas require further capacity-building support in South-Eastern Europe and how the OSCE should support the participating States in other sub-regions, namely Central Asia, Eastern Europe and South Caucasus. It will also debate what new trends in digital technologies may impact cybercrime in the foreseeable future, including potential implications of the artificial intelligence for the work of law enforcement, and how to ensure complementarities and synergies between the OSCE and other key multilateral actors active in this field such as the Council of Europe or UNODC.

Draft Agenda

Conference Venue: *The Federal Ministry of the Interior of the Republic of Austria (Großer Vortragssaal), Minoritenplatz 9, 1010 Vienna*

08:45-09:15 Registration

09:15-10:00 Opening session

10:00-11:15 Session I – Setting the scene: crime in the digital era

- Which features do make cybercrime an increasingly potent threat for our societies?
- What unique challenges does cybercrime pose for criminal justice system?
- How should criminal justice institutions respond to the growing threats posed by cybercrime?
- What assistance can multilateral organizations provide to enhance national capacities in investigating and prosecuting cybercrime?

11:15-11:30 Coffee break

11:30-12:45 Session II – Responding to the challenge: effective capacity building

- What are key elements of effective capacity building for criminal justice institutions combating cybercrime?
- What are most common challenges when implementing capacity-building programs and projects in this area?
- How to ensure long-term sustainability and local ownership of capacity-building assistance?

12:45-14:00 Lunch break

14:00-15:15 Session III – Taking the stock: OSCE's regional initiative on combating cybercrime in South-Eastern Europe (2017-2019)

- What are key outcomes of the OSCE's regional cybercrime initiative implemented in South-Eastern Europe in 2017-19?
- What were main achievements and main challenges when implementing training activities at both the regional and national levels?
- What are key lessons learned for building national training capacities in this area?

15:15-15:30 Coffee break

15:30-17:00 Session IV – Looking ahead: future OSCE's activities in combating cybercrime

- What thematic areas require further capacity-building support in South-Eastern Europe?
- How should OSCE support its participating States in other sub-regions of the OSCE area, namely Central Asia, Eastern Europe and South Caucasus?
- Which new trends in digital technologies may impact criminal activities in the future? What impact may developments in artificial intelligence have for the work of law enforcement in this regard?
- How to ensure complementarity of the OSCE's activities in the area of cybercrime with other key international players such as the Council of Europe?

17:00 Closing remarks