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

24 May 2019
Austrian Federal Ministry of the Interior, Vienna

KEY FINDINGS AND OUTCOMES[1]

[1] For more detailed account of the event, please refer to the conference report.

Introduction

The conference *"Crime in the Digital Age: Enhancing Capacities of Criminal Justice Institutions across the OSCE Area"* was organized by the Strategic Police Matters Unit of the OSCE Secretariat's Transnational Threats Department (TNTD/SPMU), in close co-operation with the 2019 Slovak OSCE Chairmanship and the Austrian Federal Ministry of the Interior. The event was the concluding activity of the OSCE's flagship regional capacity-building project on combating cybercrime and cyber-enabled crime in South-Eastern Europe implemented since the summer 2017.[2] The conference contributed to the current discussion on how to address the growing threats posed by this phenomenon by focusing on four specific issues: (1) key challenges posed by cybercrime and cyber-enabled crime for the criminal justice system and potential responses, (2) main elements for effective capacity building in this area, (3) outcomes and lessons learned from the implementation of the OSCE's regional project in South-Eastern Europe in 2017-19, and (4) future trends and OSCE's engagement in combating cybercrime.

1) Challenges posed by cybercrime and cyber-enabled crime for criminal justice

- Investigating and prosecuting cybercrime and cyber-enabled crime poses three main types of challenges:

  (1) **technical challenges:** complicated identification of perpetrators in the virtual space due to various anonymization and encryption tools, problematic retention of electronic evidence due to the volatile nature of electronic data, and volume of data that potentially needs to be analyzed;
  (2) **legal challenges:** legal limitations for investigation and prosecution in the virtual world much more restrictive than in the physical world, administratively cumbersome and lengthy mutual legal assistance (MLA) requests for cross-border access to electronic evidence, legal frameworks do not reflect latest technological developments;
  (3) **knowledge gap**: specific knowledge needed on behalf of all criminal justice practitioners, a fast-evolving phenomenon that requires a constant update of knowledge and skills.

- The **protection of fundamental rights** should be treated equally in both physical and virtual worlds. Criminal justice institutions should have the same powers when investigating and prosecuting crimes in the virtual space as they have in the real world, in particular with regard to access and retention of (electronic) evidence.

- **Adequate legislative frameworks** are necessary for effective investigation and prosecution. In particular, criminal law, law of criminal procedure and administrative law need to be amended to reflect the growing role of electronic evidence and new trends related to cybercrime/cyber-enabled crime. Due to the constant development of digital technologies, the laws should be written in **technologically neutral way** to the maximum extent possible so they can stand the test of time.

- **More effective cross-border access to electronic evidence** needs to be ensured, in particular through more streamlined process for the MLA requests. Instruments that can help facilitating MLA in a more effective way include multilateral online platforms for

[2] The OSCE extra-budgetary project No. 1101901 "Capacity Building for Criminal Justice Practitioners Combating Cybercrime and Cyber-enabled Crime in South-Eastern Europe".

secure exchange of electronic evidence and communication among criminal justice institutions, professional networks of criminal justice practitioners (national, regional, and international), practical guides and glossaries in national languages on making MLA requests, and enhanced co-operation with the Internet Service Providers.

- Further **improvement of international standards** for data retention as well as handling of electronic evidence and harmonization of legislation in this area among states would further simplify the MLA process.

- It is necessary to provide **continuous education on this topic to all criminal justice practitioners**, including judges. Relevant national training institutions (police academies, prosecutors' training centers and judicial academies) need to include this subject into their standard teaching curricula.

- Combating threats posed by cybercrime and cyber-enabled crime requires shift in the mindset and approach of criminal justice practitioners from "do-it-yourself" to "**do-it-together"** and from "need-to-know" to **"need-to-share"** knowledge and responsibilities.

- Given the transnational nature of the threats emanating from the cyberspace, **international organizations play particularly important role** in several areas: raising awareness; identifying and analyzing key trends, problems and challenges; providing a platform for the exchange of best practices and lessons learned; developing proposals for new multilateral tools and solutions; providing technical assistance and capacity-building support to criminal justice institutions; and developing and maintaining tools to facilitate international co-operation.

2) Elements for effective capacity building in combating cybercrime

- Enhancing capacities to combat cybercrime/cyber-enabled crime needs to be included among **priorities of national cybersecurity strategies** and requires corresponding action plans to be developed by all criminal justice institutions.

- Building capacities of criminal justice institutions needs to be accompanied by **development of domestic cybercrime legislation** based on relevant international standards and norms.

- **Collaboration and partnerships between public and private sectors** are of paramount importance. It is necessary to further enhance co-operation between criminal justice institutions on one hand, and academia as well as private sector on the other. The key areas for co-operation include research, innovation, training and education, exchange of information and technical solutions, and sharing of best practices and lessons learned.

- Combating cybercrime/cyber-enabled crime requires **diverse teams** that involve experts with different kinds of IT knowledge and skills and experts with investigation experience. Criminal justice institutions should adopt **special HR measures and incentives to retain staff** with IT knowledge and skillset and **prevent their move** to private sector or re-assignment to a different field. It is also important to develop and introduce standard operating procedures and provide relevant units with necessary hardware and software equipment.

- When addressing the knowledge gap among criminal justice practitioners, it is necessary to shift focus from providing training to building **long-term and sustainable education**

on this subject. This needs to be reflected in the approach of relevant national training institutions. Standard teaching curricula for various profiles within the criminal justice system need to be amended to include basic education on this subject for all practitioners and more specialized education for specific roles.

- Capacity building should not be limited only to an isolated department or unit but should be targeting an entire organization/institution, and gradually the entire criminal justice system. However, different actors require different levels of knowledge, depending primarily on whether they have managerial, investigative or technical role. It is recommended that **cybercrime education is standardized around standard job roles and skills**.

- All criminal justice practitioners need at least basic education to understand key concepts, methods and processes. However, different practitioners have different educational needs and training content needs to be tailored to their profile and role. Training involving various practitioners is advisable only for the basic introductory level.

- **Training-of-trainers** (ToT) is an effective approach for cascading knowledge to a wider number of practitioners and achieving more sustainable results. ToT programme should be always accompanied by **development of training material** for relevant national training institutions to ensure real long-term sustainability.

- In terms of training development and delivery, a **balance between theory and practice** needs to be ensured. **Scenario-based exercises** inspired by real cases and **exercises requiring collaboration** are most effective for reinforcing learning. It is recommended to deliver as much theory as possible in the form of pre-read/pre-course material, ideally via an e-learning platform. The use of native speakers as trainers whenever possible is also advisable.

- Training content should be always **tailored to local legislative environment, existing technical infrastructure, work culture and practices, and level of knowledge**. If possible, pre-assessment of trainees with regard to their existing knowledge and experience should be always conducted beforehand.

- **Raising public awareness** about cybersecurity in general, and cybercrime in particular, needs to be an integral part of a long-term strategy to address challenge emanating from the cyberspace.

3) Lessons learned from the OSCE's regional project in South-Eastern Europe

- There is an **urgent need for basic training** on electronic evidence and introduction to cybercrime/cyber-enabled crime for vast majority of police officers and investigators in the region. The national training activities initiated by the OSCE's project represent a first important step. However, cascading the knowledge to even wider number of police officers will require further and more long-term efforts. The countries in the region should develop their own **national training strategies** for cybercrime and electronic evidence for various criminal justice institutions.

- Regional training activities have many advantages but they can never fully suit specific needs of each beneficiary country. It is a good practice if a **regional project involves also activities at the national level** that can be tailored to needs and context of each beneficiary country.

- For practitioners outside specialized units who need only basic or intermediate knowledge, **training by local experts from specialized units** is particularly appreciated as it can be delivered in a national language and tailored to the needs and context of each country.

- **Co-operation between police training institutions and operational units** is necessary for building up national education on cybercrime. However, with limited capacities of the operational units for conducting training, the police training institutions across the region need to gradually build their own capacities (especially in terms of ensuring sufficient number of qualified lecturers) so they can co-ordinate and steer education of the police on this subject in the long term.

- Training-of-trainers programme and development of a course on handling electronic evidence in various national languages of South-Eastern Europe were identified as crucial for long-term sustainability of the project's results. There is **need to develop more curricula on cybercrime-related topics** in national languages of South-Eastern Europe for basic and supplementary police training in the future.

- Police training institutions across the region face **lack of adequate technical equipment**. Future capacity-building projects need to include also procurement of IT equipment, so the training institutions have the necessary means to meet the growing need.

- While not a primary target group for this project, **judges were the most difficult to engage** in regional training activities. More consideration needs to be given to specific ways and methods of engaging judges on this topic. For regular police investigators, more joint training courses with prosecutors may be beneficial.

4) Outlook for the future

- Cybercrime has been gradually evolving into a consolidated, well-run and efficient **business model**. In particular, "**cybercrime-as-service**" industry has marked considerable growth over the recent years. **Financially-motivated malware attacks**, in particular **ransomware**, remain the dominant form of cyber-dependent crime. This is unlikely to change in the foreseeable future. **Social engineering**, primarily via phishing e-mails, plays increasingly important role in facilitating many cyber-dependent and cyber-enabled crimes and can be expected to become even more sophisticated and targeted in the future.

- Market places on the **Darknet** will continue facilitating trade in illicit goods and services. With shutting down of some major market places, smaller and more decentralized market places emerge, often targeting specific language groups or nationalities. Some users also move to entirely different platforms such as various encrypted communication applications, complicating further efforts of law enforcement to identify perpetrators. The Darknet is also becoming increasingly used for distribution of extreme child sexual exploitation material, although majority still remains to be shared through peer-to-peer (P2P) platforms. With the growing popularity of social media applications, the growing amount of self-generated explicit material is live streamed.

- Criminals and organized criminal groups are increasingly misusing **cryptocurrencies** to fund their activities and also launder illicit profits. Bitcoin remains the main cryptocurrency encountered by law enforcement although new currencies are also gaining

ground (e.g. Zcash, Monero). Cryptocurrency users and facilitators are becoming victims of cybercrime as well. A new emerging trend is **cryptojacking**.[3]

- The evolving technology that may have most significant impact on criminality in the future is **development of artificial intelligence** (AI). The **potential misuse of AI for criminal purposes** involves: increased effectiveness of cyberattacks through development of more sophisticated and advanced tools (e.g. automation of social engineering attacks or automation of hacking); delivering physical attacks by autonomously operating systems; conducting political attacks through fabricating and spreading realistically-looking fake news and fake videos.

- At the same, it should be recognized that **AI offers also opportunities** for improving the work of criminal justice institutions. Its potential use includes: more precise face recognition and identification of persons of interests in crowded spaces; analysis of large amount of audio/video data; prediction of crime trends allowing for more effective and efficient allocation of resources; identification and removal of online hate speech and terrorism-related content; detection of suspicious sounds, behaviors and anomalies; or enhancing resilience of cyber infrastructure.

- Another technology that can have potentially significant implications in the future is **quantum computing**. In the context of criminality, potential ability of quantum computers to dissolve all modern encryption methods currently used for ensuring Internet safety and cybersecurity is most worrisome.

- When it comes to misuse of modern technologies for criminal purposes, state institutions face **scalability problem**. Even if they build capacities to effectively address these new forms of crime, their mere volume may be simply too overwhelming to manage. Capacity building therefore needs to be combined with **adequate policy responses** that can influence **factors at the macro level**. Criminal justice systems are currently designed on reactive case-based/offenders-based models. This needs to be supplemented with **larger market-based responses**.

- The OSCE should focus its efforts primarily on assisting its participating States with **addressing technical challenges and knowledge gap**. Need to continue close co-ordination and co-operation with other key players in this area such as CEPOL, Council of Europe, Europol, INTERPOL, and UNODC was underlined.

- In **South-Eastern Europe**, the OSCE should build on the outcomes of its regional project implemented in 2017-19. In particular, it should further strengthen capacities of police training institutions to provide sustainable and long-term education on this subject, enhance capacities of digital forensic labs across the region, and raise awareness about electronic evidence and cybercrime/cyber-enabled crime among regular police officers.

- There is growing interest in capacity-building support for combating cybercrime and cyber-enabled crime also among the OSCE participating States in **Central Asia** and **South Caucasus**. The OSCE should consider developing new regional capacity-building initiatives for these sub-regions.

[3] Exploiting computer power of the Internet users for mining cryptocurrencies without their knowledge and consent.