Strategic priorities in the cooperation against cybercrime for South-East Europe and Türkiye

Co-funded by the European Union
EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Co-funded and implemented by the Council of Europe

Contents

Contact
Cybercrime Programme Office of the Council of Europe (C-PROC)
Email: cybercrime@coe.int

Disclaimer
This document has been prepared with the support of CyberSEE, a joint project co-funded by the European Union and the Council of Europe. The views expressed herein do not necessarily reflect official positions of the European Union or the Council of Europe.

Declaration on Strategic Priorities for cooperation against Cybercrime

We, representatives of Ministries of Justice, Offices of Prosecutor's General, Appellate Prosecution Office and Ministries of Interior
of States and areas participating in the CyberSEE joint project of the European Union and the Council of Europe

Meeting at the CyberSEE Steering Committee, held on 10 December 2024 in Strasbourg, France;

Considering Strategic Priorities in the Cooperation against Cybercrime adopted by the Meeting of Ministers and Senior Officials of Ministries of Interior and Security, of Ministries of Justice and of Prosecution Services of countries and areas participating in the CyberCrime@IPA project in Dubrovnik, Croatia, on 15 February 2013.

Recognising the need for revised and updated strategic priorities for cooperation against cybercrime in the South East Europe and Türkiye in light of multiple political, economic and social challenges and developments in the region and in line with European Union policy priorities in this area;

Conscious of the benefits of information and communication technologies that are transforming our societies;

Concerned by the risk of cybercrime that adversely affects confidence and trust in information technologies as well as the rights and safety of individuals, businesses and entire countries;

Recognising the positive obligation of governments to protect individuals against cybercrime;

Mindful of the need to respect fundamental rights and freedoms, including the protection of individuals with regarding to the processing of personal data, when protecting society against crime;

Considering the need for cooperation between public and private sectors for the prevention and control of cybercrime and the protection of computer systems;

Believing that effective measures against cybercrime require efficient regional and international cooperation;

Underlining the value of the Budapest Convention on Cybercrime and its related standards as a guideline for domestic legislation and a framework for international cooperation;

Noting with appreciation the increasing importance paid by the European Union to cyber resilience, cybersecurity and action against cybercrime;

Grateful for the support provided by the European Union and the Council of Europe through implementation of the CyberCrime@IPA, iPROCEEDS and iPROCEEDS-2 regional projects since 2010;

Building on the progress made and on the action on cybercrime already taken in the States and areas of the region, while noting that further efforts are required;

We endorse
the updated strategic priorities for cooperation against cybercrime
presented at this Steering Committee meeting
and
we are committed to

Keep legislation up to date, implement the Budapest Convention and the Second Additional, as applicable, that meets human rights and rule of law requirements;

Develop and update cybercrime policies and strategies to meet the new threats and challenges;

Provide continuous and sustainable training for law enforcement and judiciary;

Develop and pursue parallel financial investigations in cybercrime cases;

Enhance public private cooperation in both cybercrime and cybersecurity areas;

Use the tools provided by the Budapest Convention and Second Additional Protocol to enhance international cooperation;

Improve national inter-agency cooperation, in particular in the areas of cybercrime, cybersecurity and financial investigations;

Share our experience with other regions of the world to support capacity building against cybercrime;

Promote adherence to the Budapest Convention on Cybercrime at the global level.

Declaration adopted by acclamation in
Strasbourg, France, 10 December 2024

Appendix: Strategic priorities on cybercrime

1. Keeping legislation up to date, implementation of the Budapest Convention and the Second Additional Protocol.

Updated and adequate legislation is the basis for law enforcement action and the judiciary to take criminal justice measures against cybercrime. As electronic evidence can be part of almost any criminal investigation it is necessary to ensure possibilities for its collection, use and admissibility. During different projects countries have made progress to bring their domestic legislation in line with the Budapest Convention as well as other related Council of Europe and European Union standards, including personal data protection, protection of children agains sexual violence, as well as standards and tools related to fight against money laundering, tracing of crime proceeds, their seizure and confiscation.

However, legislation needs to be constantly checked, whether it is up to date and meets also new and emerging threats and challenges.

While the Budapest Convention has been in place since 2001, there are also new tools available to countries. In May 2022 the Second Additional Protocol on enhanced cooperation and electronic evidence was opened for signature. It is the result of years work of the Council of Europe and it aims at facilitating access to data stored in other jurisdictions as well as improving the effectiveness of Mutual Assistance. Relevant legislative and other measures at domestic level are needed to use the provisions of the Protocol.

Therefore, work on the legislation needs to continue, while taking into account human rights and rule of law requirements.

Relevant authorities should consider the following actions:

- **To continue alignment of domestic legal frameworks to accord fully with the Budapest Convention.** In order to fight cybercrime and conduct effective investigations it is necessary that domestic legislation is fully in line with the Convention while also paying respect to other requirements related to protection of fundamental rights, protection of personal data.

- **To raise awareness about the Second Additional Protocol and its tools, sign and ratify the Protocol if applicable.** The Protocol provides new tools for the law enfocement and judiciary to facilitate international cooperation and improve access to electronic evidence. Although the Protocol has been in place since 2022, it is still relevant to raise awareness about its tools and added value it would provide to countries.

- **To ratify the Protocol, develop and align the domestic legislation.** Countries are encouraged to sign and ratify the Protocol. However, it should be borne in mind that its implementation would require both legislative and other measures, changes to legislation and procedures, building necessary capacities.

- **To identify legislative gaps to deal with emerging challenges such as conduct of financial investigations, search, seizure and confiscation of criminal assets that include virtual and crypto currencies.** New and emerging challenges related to technological developments as well as changes in cybercrime and its modus operandi require adequate response from the law enforcement and judiciary. However, in case there are gaps and existing regulations cannot be applied, legislative and other measures need to be taken. Governments need to ensure that domestic legislation meets those challenges and can be effectively used.

2. Continue to develop cybercrime policies and strategies in order to meet the new threats and challenges

The developments related to information and communication technologies, introduction of new digital solutions and services, require that governments prioritize ensuring their security. Cybersecurity and cybercrime policies and strategies have been developed to ensure coordinated approach, engagement of all relevant stakeholders and having both short-term and long-term objectives. It is the task of the governments to take legislative and other measures to protect people from various cyber threats including cybercrime. Governments may develop both cybercrime and cybersecurity strategies and action plans. However, in case the wish is to continue only with cybersecurity strategy, it must be ensured that it contains criminal justice and cybercrime component. Due to development of technologies as well as changes in global security and cybersecurity, policies and strategies together with action plans need to be periodically reviewed and updated.

Governments should consider the following actions:

- **To develop domestic cybercrime and cybersecurity strategies supported with action plans.** Policies and strategies on both cybercrime and cybersecurity are needed in order to coordinate activities, have a whole-of-government approach and set long-term and short-term objectives. It is important that these documents would also have an action plan or roadmap, to plan activities, designate tasks and responsibilites and set deadlines for the implementation.

- **Where there is only a domestic cybersecurity strategy, to ensure that it contains both a cybercrime and criminal justice component.** Often countries do not have a separate cybercrime strategy, but have chosen to develop and adopt national cybersecurity strategy. In this case governments need to ensure that cybersecurity strategy contains also cybercrime and criminal justice components and addresses fight against cybercrime, competent authorities, their needs and resources.

- **To develop domestic policies and strategies, supported by action plans that aim to prevent, detect and prosecute cybercrime offences and raise national capacities.** Strategies need to have also action plans or roadmaps to ensure that policies and objectives would be implemented by relevant authorities. As regards fight against cybercrime, then these documents need to address also prevention, investigations, problems and challenges identified and responses to solve or mitigate them. While planning resources and investments for cybersecurity, particular attention should be paid also to the needs on law enforcement and judiciary.

- **Cybercrime policies and strategies should seek to define, drive and measure the improvements and performance made in relevant agencies in response to cybercrime.** Policies and strategies need to reviewed on a periodical basis and implementation assessed. Monitoring the implementation should take place during the whole strategy period. In case certain objectives are not fulfilled and activities not carried out, these should be addressed during the next phases.

- **Cybercrime strategies should align with domestic cybersecurity strategies as well as other sectoral strategies such as on serious and organized crime, anti-money laundering etc.** Fight against cybercrime is closely related to other crimes and criminal investigations. Cybercrime offences may be related to other serious crime or organised crime. More often we can see how cybercrime is related to money laundering offences. Therefore governments need to ensure that all such sectoral policies and strategies are not in conflict, but instead complement each other.

3. Continuous and sustainable training

Effective implementation of policies and strategies as well as legislation requires that governments establish necessary capacities. One of the most relevant elements here is the training of LEA officers, prosecutors, and the judiciary.

The rise of number of cybercrime offences, their increased complexity, changes in modus operandi, use of new technological solutions and tools requires that governments ensure continuous and sustainable training of both law enforcement and judiciary.

As the use of information and communication technologies has become part of modern everyday life, it has also resulted in a situation where electronic evidence can be part of almost any criminal investigation. This in turn requires that not only officers involved in cybercrime investigations, but also other law enforcement officers, including first responders receive basic training on electronic evidence.

The complexities of technology, digital devices, and electronically stored data need to be understood by prosecutors and the judiciary in order to lead, and fairly adjudicate cases where electronic evidence is relevant. Decision making in the search, seizure, and confiscation of electronic evidence and data that represents financial value (such as virtual payment systems) are an ever increasing subject for all courts in all countries.

As cybercrime has become more complex, new technologies have brought additional cybercrime modus operandi and typologies, different tools are available for anonymisation and encryption, increased use of virtual or crypto currencies, training strategies and programs must keep the pace and ensure that effective investigations can be conducted. Cross-border nature of cybercrime, need to obtain electronic evidence from abroad mean that trainings need to focus also on different aspects of international cooperation.

As national training institutions are key partners to ensure that such programmes are available and offered to an increasing number of criminal justice professionals, strengthening capacities of such institutions and their ownership of cybercrime and electronic evidence remains a strategic priority.

Governments should consider the following actions:

- **To develop and publish domestic training strategies in relation to electronic evidence and cybercrime investigations for law enforcement agencies, prosecutors and the judiciary**. According to the benchmarking of current capabilities and capacities assessed in the iPROCEEDS-2 end of project report, further training is needed by all project countries. However, there are also some strengths in the project countries that need less development. A holistic training plan would identify long-term and short-term objectives, whilst putting in place sustainable means of provision of training and a clear plan of delivery. It is important that any strategy puts in place sustainable training, through delivery by existing training Centres and the roll out of material through trained trainers.

- **Trainings on new and emerging cybercrime threats and challenges should be provided to law enforcement agencies, prosecutors and the judiciary**. New and emerging cybercrime threats such as dark web, cryptocurrencies, other virtual payment systems and the criminal development and use of malware is bringing numerous challenges to the investigation and prosecution of cybercrime. The awareness of, prevention from, and investigation of these crime types remains crucial to protect the public from advanced cybercriminals. Intermediate and advanced

training courses (including scenario-based training) is necessary to prepare the authorities in the region to counter these threats and risks.

- **Trainings focussed upon inter-agency cooperation should include topics related to financial investigations, and partnership working with the FIU-s and CERT/CSIRT**. Inter-agency cooperation in country between stakeholders takes place successfully in most European countries. Such collaboration has provided demonstrable success in intelligence sharing and cooperation to reduce the impact of cybercrime, as well as providing significant opportunities to interdict offenders, prevent further harm, and confiscate proceeds of crime. Inter-agency cooperation has been a constant feature of previous projects. Currently, inter-agency cooperation generally takes place when a legal request is made in relation to a specific investigation. Outside of these processes, little inter-agency information sharing and cooperation occurs outside of relies upon either an ad-hoc sharing process or on an. Improved partnership working, in collaboration with training activities, should see similar improvements that are reported elsewhere in Europe.

- **Trainings on international cooperation, in particular in light of the Second Additional Protocol and its tools**. The Second Additional Protocol provides new tools for the law enforcement and judiciary to facilitate international cooperation and improve access to electronic evidence. Where legislation is being drafted in support of the accession of this protocol, the understanding of these new tools and the international dimensions is crucial. Planning and delivery of training courses (including scenario-based training) will prepare officers to allow for the early use of tools in the fight against cybercrime.

- **To ensure that countries are able to sustain training capabilities through the continual development of a caveat of national trained trainers for law enforcement agencies, prosecutors, and the judiciary**. Trained trainers should regularly deliver training courses to prevent the lapse of their skills. Statistics about the number of courses that they deliver, and the students trained, should be collated to demonstrate a measurable return on investment.

4. Continuous development in parallel financial investigations in cybercrime cases

Cybercrime and other offences are mostly aiming at financial gain. Cybercrime, online fraud and other forms of economic and serious crime can generate lot of economic profit for the criminals. Crime proceeds are also often related to money laundering offences as criminals try to convert and transfer the proceeds between different jurisdictions. The use of virtual and crypto currencies have been used more often to conceal the origin or ownership of the proceeds.

In addition to cybercrime investigations, parallel financial investigations have become relevant to identify, trace, seize and confiscate crime proceeds. It is necessary to address measures for the prevention of fraud and for the prevention and control of money laundering on the Internet.

Governments should consider the following actions:

- **To review the legislation and procedures for cooperation and information exchange to ensure effective financial investigations in parallel to the criminal investigations**. To effectively counter the financial motivation for most cybercrime, governments must recognise that they must be prepared to put in place effective legislation to search for, seize, and confiscate criminal property. Reviewing

current legislative capabilities and introducing new legislation to counter any shortfalls, will enable effective parallel financial investigations in cybercrime cases, especially where cryptocurrencies and virtual assets are relevant to the matters.

- **Ensure necessary training on financial investigations and tracing, seizure and confiscation of virtual and cryptocurrencies**. The growing criminal use and abuse of cryptocurrencies, and other virtual payment systems provides numerous challenges to the search, seizure, and confication of criminal property. Training courses are needed to proovide capabilities in Financial Investigation Units, Financial Intelligence Units and other to counter these challenges. Where appropriate the training should compliment legislation and prepared best practice guidelines.

- **To improve the detection, seizure, and confiscation of (cyber)crime proceeds, including virtual currencies**. It is necessary to continually develop capabilities in the tracing of proceeds of crime (including cybercrime). Investigating how cybercriminals launder, conceal, and spend the proceeds of crime is an important step, expected by all communities. Additional domestic capacity building to investigate blockchain technology, crypto currencies, stablecoins and other virtual currencies through the implementation of training, guidelines and best practice are needed to compliment traditional financial investigation methods.

- **Increase the number of parallel financial investigations in cybercrime cases.** Financial gain remains the key driver in cybercrime. Recognition of the large gains and losses as a consequence of cybercrime is vital, and taking appropriate steps to target financial gains and the seizure of criminal property should be a priority. Implementation of key performance indicators or other statistics may help to measure the increased activity during parallel financial investigations.

- **Improve cooperation with Asset Recovery Offices and Financial Intelligence Units**. Asset Recovery Offices (ARO's) are being established in the region to support conviction and non-conviction-based processes for the detection, recovery, and confiscation of the proceeds of crime as a consequence of recommendations by the MONEYVAL Committee. Building on earlier successes, it would be advantageous if the countries in the region enhance relationships with the new ARO's and Financial Investigation Departments and Financial Intelligence Units through intelligence sharing agreements and memorandums of understanding. With the anticipated rise in the confiscation of assets from cybercrime and the use of virtual payment systems, countries should consider extending the current scope of information sharing agreements and collaboration.

5. Continue to enhance public-private cooperation in cybercrime and cybersecurity matters

The prerequisite of effective cybercrime investigations is trust and good cooperation between public and private sector. Often electronic evidence related to cybercrime or other crime are stored by different Service Providers, including telecommunication and Internet Service Providers. More and more there is a need to rely on other Online Service Providers, including information society services.

This also means that there is sufficient and clear legislative framework on procedural powers of law enforcement on one hand, and rights and obligations of Service Providers on the other. It is important to bear in mind the human rights, personal data protection and rule of law requirements. The public interests as well as rights and freedoms of the individuals need to be balanced. Authorities have also additional options to build trust and facilitate cooperation by

concluding cooperation agreements, memorandums of understanding, and to organise joint meetings and trainings.

Governments should consider the following actions:

- **Improve the use of public-private cooperation in cybercrime cases and where electronic evidence is sought.** Further collaboration between public and private sectors is a forward-thinking response in combatting cybercrime and collecting electronic evidence. Currently, in many countries public-private cooperation is based upon requests and orders for information on a case-by-case basis rather than a regular exchange of informaiton. Often, private sector is also able to support and provide information on an informal basis, which can support LEA and Prosecutors to quicker and more efficinetly acquire evidence in investigation of cybercrime as well as establish the location of electronic evidence.

- **Increase the volume and quality of two-way exchanges of information and intelligence to prevent and detect cybercrime.** Both the private sector and LEA would also benefit from more information sharing about cases, trends and threats from cybercriminal. This supports cyber-security, investigation, and prevention strategies to evolve more efficiently, ensuring more tangible results in combating cybercrime. To measure the success of this action, some statistics will be required to measure its effectiveness or otherwise.

- **Seek improvements and cooperation between project countries and Online Service Providers**. Where necessary, such improvements should include hosting services, cloud services and alike. Countries need to strengthen cooperation between relevant stakeholders, such as ISP's, Communication Service Providers and Virtual Asset Service Providers at the domestic, regional and international lever. Other relevant stakeholders include service providers that host websites, store data and provide cloud services, where electronic evidence is often found, where it is particularly necessary to improve cooperation as their resources are used more to store data likely to become relevant to criminal investigations.

- **To ensure that relevant legislation and procedures relating to public-private cooperation are effective.** Where legislation is required to underpin sharing of information and electronic evidence between public and private sectors, it is important that the legal framework is reviewed, and improvements made when necessary. Where information is shared on an ad-hoc basis or through agreements, the effectiveness of MOU's and information sharing agreements should be reviewed and improved where necessary.

6. Improve national inter-agency cooperation

The complexity of cybercrime offences, their relation to cybersecurity and financial investigations, require that there is a good and effective cooperation between law enforcement and other government authorities. Often cybersecurity incidents can be considered also as cybercrime offences and this requires close cooperation and coordination by law enforcement and cybersecurity authorities. It is necessary that law enforcement and CERT/CSIRT exchange information about cyber risks and threats and if necessary coordinate actions in case of investigations. Both can also engage in training and awareness raising activities as implementation of cybersecurity measures and knowledge about the risks can also contribute to cybercrime prevention.

Financial investigations parallel to criminal investigations also require that law enforcement authorities cooperate and exchange information with Financial Intelligence Units (FIU) and

Asset Recovery Offices (ARO). During the investigation which is related to causing financial loss to a victim and converting and transfering crime proceeds, different opportunities need to be used, including those provided by FIUs and AROs, to trace and recover crime proceeds.

Governments should consider the following actions:

- **Improve cooperation with other government authorities to ensure information exchange and effective access to electronic evidence, including law enforcement, FIU-s and CERTs/CSIRTs**. The complex nature of cybercrime and as well as other crime involving electronic evidence require close and effective cooperation with other national authorities whose main task may not be conduct of criminal investigations. As often criminal offences, including cybercrime are being committed for financial gain or economic profit, additional steps and efforts are needed to track criminal proceeds for the purposes of seizure, confiscation of return to victims. Authorities or units responsible for financial investigation, detection and recovery of property need to be engaged in parallel to the criminal investigations. As regards FIUs, then they have additional powers provided by the legislative framework which enable them to cooperate with financial institutions, order suspension of transactions, freezing bank or payment accounts. When cybercrime involves attacks against government or critical information infrastructure, cybersecurity authorities, CERT/CSIRT need to be involved in the process.

- **Introduce and implement legal frameworks and/or Memorandum of Understanding (as necessary) to increase information sharing and cooperation between law enforcement agencies and CERT/CSIRT bodies**. Governments need to ensure that legislative framework enables such intra-agency cooperation and there are no obstacles for information exchange. In order to facilitate cooperation, agreements and MoUs could be introduced to coordinate and agree on technical details concerning cooperation, including contact person, information exchange channels etc.

- **Improve inter-agency cooperation between public departments charged with the prevention, detection and prosecution of cybercrime cases**. Due to the evolving nature of cybercrime and other crime involving electronic evidence, increase in their volume and complexity, it is important that all relevant stakeholders or authorities are involved in planning and implementing crime prevention, analysing the needs and challenges related to detection, investigation and prosecution of cybercrime. In case of gaps in legislation or deficiencies concerning procedures and capacities, all relevant authorities need to take coordinated action, including changes to legislative or organizational frameworks as well as building additional capacities.

7. International cooperation

As most of the cybercrime as well as crimes involving electronic evidence have become cross-border, cybercrime and electronic evidence can be considered both transnational by nature. Even if the case or investigation is of domestic nature, electronic evidence needed could be stored abroad by different jurisdictions. For cybercrime investigations and investigations involving electronic evidence it is crucial secure and obtain evidence as fast as possible.

However, there are still different obstacles related to Mutual Assistance, in particular the bureaucracy needed and overall speed and effectiveness.

While the Budapest Convention relies on mutual assistance, exchange of spontaneous information and the work of the 24/7 network, the Second Additional Protocol provides new additional tools to expedite international cooperation and access to electronic evidence.

Governments should consider the following actions:

- **Continued and increased use of the Budapest Convention 24/7 Point of Contact.** As cybercrime and also other criminal investigations involve electronic evidence which is often stored in other jurisdictions, countries need to use extensively international cooperation. Countries need to ensure that its one or more 24/7 Point of Contact are well equipped, trained and are able to use all available international cooperation tools.

- **Continued and increased use of other Budapest Convention tools, relating to international cooperation including the use of Mutual Assistance and spontaneous information**. Budapest Convention can be used as legal basis for international cooperation and provides range of tools for that purpose. Countries are encouraged to use these tools to the widest extent possible. In addition to Mutual Assistance related to requests and responses to them, spontaneous information should be used more. Spontaneous information as a measure and provision of information to another country without it's prior request can build mutual trust as well as strengthen international response to cybercrime.

- **Implementation of legislation and of the tools provided in the Second Additional Protocol.** The Protocol provides a set of additional tools, including direct cooperation with Service Providers and measures to facilitate and speed up Mutual Assistance. Countries are encouraged to sign and ratify the Protocol. Governments need to ensure that once ratified the Protocol, there are necessary legislative and other measures in place as well as capacities and training needed for its implementation.

- **Support activities related to improvements and more effective cooperation with Multinational Service Providers.** Multinational Service Providers continue to play an important role in international cooperation. While cooperation on a voluntary basis can take place already now, the Protocol would provide also clear and binding legislative framework. Governments should continue cooperation and dialogue with the Multinational Service Providers and identify options for a better and more effective cooperation. Cooperation agreements and MoUs as well as the use of templates agreed prior would definetely complement to this objective.
- **Use international workshops, conferences and meetings to improve the productivity and timeliness of international cooperation.** One of the keys to effective international cooperation and investigations is trust and networking. Therefore, governments and authorities are encouraged to participate actively in different regional and international meetings such as conferences, working groups and roundtables. Joint regional and international trainings are also very important and help to build culture of cooperation.