CyberEast

Strategic Priorities for Cooperation on Cybercrime in the Eastern Partnership Region

Adopted within the context of the
Octopus Conference on Cybercrime
14 December 2023, Bucharest, Romania

Bucharest, 14 December 2023

www.coe.int/cybercrime

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 CyberEast, 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 on Cybercrime

We, representatives of Ministries of Interior and Security,
Ministries of Justice and Offices of Prosecutor's General
of States participating in the CyberEast joint project of the European Union
and the Council of Europe

Meeting at the Octopus Conference on Cybercrime, held from 13 to 15 December 2023 in Bucharest, Romania;

Considering the Strategic Priorities for the Cooperation against Cybercrime in the Eastern Partnership Region Adopted at the Conference on Strategic Priorities under the CyberCrime@EAP project, Kyiv, Ukraine, 31 October 2013;

Taking note of the Joint Communication to the European Parliament, The European Council, The Council, the European Economic and Social Committee and the Committee of the Regions on the Eastern Partnership policy beyond 2020: Reinforcing Resilience – an Eastern Partnership that delivers for all and Council of the European Union Conclusions on Eastern Partnership policy beyond 2020;

Recognising the need for revised and updated strategic priorities for cooperation against Cybercrime in the Eastern Partnership Region 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@EAP and CyberEast regional projects since 2011;

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

We endorse
the updated strategic priorities for cooperation on cybercrime
presented at this Conference
and
we are committed to

Pursue informed cybercrime strategies to ensure an effective criminal justice response to offences against and by means of computers as well as to any offence involving electronic evidence;

Adopt complete and effective legislation on cybercrime, in line with the Budapest Convention on Cybercrime and its Protocols, as applicable, that meets human rights and rule of law requirements;

Establish effective and accessible cybercrime reporting systems that allow for the general public and the private sector to report cybercrime securely;

Pursue public awareness campaigns and other actions that increase awareness and understanding of cybercrime threats and responses;

Support the strengthening of national law enforcement and judicial institutions that are offering training on cybercrime and electronic evidence;

Promote financial investigations and the prevention and control of fraud and money laundering on the Internet;

Improve international and public-private cooperation on cybercrime and electronic evidence in view of requirements of the Second Additional Protocol to the Budapest Convention, as applicable;

Facilitate coordinated responses to cyber threats through cooperation between cybersecurity experts and criminal justice authorities;

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
Bucharest, Romania, 14 December 2023

Appendix: Strategic priorities for cooperation on cybercrime

1. Strategic priority: Informed cybercrime policies and strategies

As societies are transformed by information and communication technology, the security of ICT has become a policy priority of many governments. This is reflected in the adoption of cybersecurity strategies by most of the region’s governments with a primary focus on the protection of critical information infrastructure. However, governments also have the positive obligation to protect people and their rights against cybercrime and to bring offenders to justice. The Cyber Barometer Studies undertaken by the CyberEast project in the region’s countries in 2021/2022 confirm a strong need for connected and informed policies that take into account threats and challenges of cybercrime, as perceived by the general public and the business sector.

Governments may therefore consider the preparation of specific cybercrime strategies or to enhance cybercrime components within cybersecurity strategies or policies.

Relevant authorities may consider the following actions:

- **Keep cybercrime policies or strategies up to date** with the current landscape of threats and challenges, aiming to ensure an effective criminal justice response to offences against and by means of computers as well as to any offence involving electronic evidence. The content of such strategies should be, where possible, informed by relevant studies and data supporting policy decisions and prioritising the needs of crime victims.

- **Ensure that human rights and rule of law requirements are met** when taking measures against cybercrime. The rights of cybercrime victims and vulnerable groups, including women and children, should be recognised.

- Wherever possible, facilitate research and partnerships with academic, scientific and other interested communities to study criminal offenders, crime groups and vulnerable persons to better inform policy decisions. Partnership with Europol and other actors involved in cross-border cybercrime research should be pursued.

- **Evaluate on a regular basis the effectiveness of the criminal justice response to cybercrime and maintain statistics**. Such analyses would help determine and improve the performance of criminal justice action and allocate resources in an efficient manner.

2. Strategic priority: Legislative alignment with the Budapest Convention and its Second Additional Protocol[1]

Adequate legislation is the basis for criminal justice measures on cybercrime and the use of electronic evidence in criminal proceedings. States participating in the joint European Union and Council of Europe projects have made much progress in bringing their legislation in line with the Budapest Convention as well as related Council of Europe and European Union standards on data protection, on the protection of children against sexual violence or on crime proceeds and money laundering.[2] However, further strengthening is required and often legislation has yet to stand the test of practice. This is particularly true for specific procedural law powers, implementation of which remain a challenge to be addressed in most of region's countries.

In May 2022, the Second Additional Protocol to the Budapest Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence was opened for signature. The Second Protocol responds to challenges and complexities of obtaining electronic evidence that may be stored in foreign, multiple, shifting or unknown jurisdictions. It does so by providing tools for enhanced co-operation and disclosure of electronic evidence that are subject to a system of human rights and rule of law, including data protection safeguards. Relevant domestic legislation and of other measures should be adopted to operationalise the provisions of the Protocol.

The adoption of complete and effective legislation that meets human rights and rule of law requirements remains a strategic priority.

Relevant authorities should consider the following actions:

- **Further improve procedural law provisions to secure electronic evidence by law enforcement.** This should include laws and implementing regulations on the use of the expedited preservation provisions of the Budapest Convention, but also other rules on access to data held by private sector entities. Full implementation of all procedural powers available under the Convention, subject to conditions and safeguards in line with Article 15 Budapest Convention, remains a key factor for both domestic investigations as well as international cooperation.

- **Implement enhanced tools for international cooperation on cybercrime and electronic evidence as provided by the Second Protocol, as applicable.** The tools of the Second Protocol include direct co-operation with service providers in other Parties for the disclosure of subscriber information and with registrars for domain name registration information; government-to-government co-operation for the production of subscriber information and traffic data; expedited disclosure of data and co-operation in emergencies; joint investigation teams and joint investigations; video conferencing. These tools are backed up by data protection and other safeguards that need to be implemented as well.

- **Evaluate the effectiveness of legislation.** The application in practice of legislation and regulations should be evaluated on a regular basis. Statistical data on cases investigated, prosecuted and adjudicated should be maintained and the procedures applied should be documented.

[1] As applicable, since not all States have signed the Second Protocol so far.

[2] See for example Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108), the "Lanzarote Convention" on the Sexual Exploitation and Sexual Abuse of Children (CETS 201), Convention on the Laundering, Search, Seizure and Confiscation of Proceeds from Crime and the Financing of Terrorism (CETS 198).

- **Strengthen data protection legislation in line with international and European standards.** Governments are encouraged to ensure that their national data protection legislation complies with the principles of the Council of Europe's data protection convention ETS 108 and to participate in the Convention's current modernisation process. The same applies to the future data protection standards of the European Union. This will facilitate the transborder sharing of data also for law enforcement purposes.

- **Complete legislation and take preventive and protective measures on the protection of children against online sexual violence**. While many provisions of the Lanzarote Convention have been implemented, in some States or areas issues such as "possession of child pornography", "knowingly obtaining access" and "grooming" still need to be addressed.

- **Adapt legislation on financial investigation, the confiscation of crime proceeds and on money laundering and the financing of terrorism to the online environment**. Rules and regulations should in particular allow for swift domestic and international information exchange.

3. Strategic priority: Effective and accessible cybercrime reporting

Cybercrime and electronic evidence require a timely and efficient response by criminal justice authorities. In many situations, existence of proper reporting systems and possibilities for the general public and business entities is a decisive factor for successful investigations and prosecutions.

However, the Cyber Barometer Studies of 2021/2022 show that cybercrime remains underreported in all of the countries of the region, without exception. Lack of online reporting portals, limited knowledge of possibilities to report, and low understanding of the threats and potential remedies all hamper proper reporting.

It should be noted that this applies to both the general public and private companies, with only large and IT-related businesses demonstrating high level of reporting.

Effective and accessible cybercrime reporting should thus become a strategic priority.

Relevant authorities should consider the following actions:

- **Establish online platforms for public reporting on cybercrime.** This should provide a better understanding of cybercrime threats and trends and facilitate criminal justice action. Such platforms may also be used for public information and threat alerts. Partnering with cybersecurity community, especially CSIRTs, who may be operating similar incident reporting solutions and systems, could be of particular value.

- **Consider use of social media and other popular channels to inform the public on the ways to report cybercrime.** Ease of use and wide availability of information on reporting can play in important role in increasing awareness and incidence of crime reporting.

- **Assign proper resources available at both law enforcement and prosecution services to tackle increased reporting and caseload.** Although all of the region's countries have established multiple law enforcement units and departments – with specialised prosecution units available in some – proper level of staffing, personnel retention, excessive workload and expenses needed to ensure specialisation remain widespread challenges. This directly contributes to lack of willingness but also limited capacities to receive and handle very high number of cases concerning cybercrime and electronic evidence.

- **Improve procedures for cybercrime investigations and the handling of electronic evidence.** Examine and consider implementation of national and international standards and good practices in this respect, from incident/crime report handling to advanced forensic analysis. Numerous standards and guidance documents developed by the Council of Europe in this area can be of support.

4. Strategic priority: Improved public awareness

The results of the Cyber Barometer Studies of 2021/2022 are unanimous and consistent in identifying general awareness of the public on cybercrime and Internet security challenges, coupled with limited action from the authorities to improve such awareness, as among the main challenges hampering action on cybercrime in the region. Most concerningly, while recognising the dangers and impact of cybercrime, many respondents from both general public and private entities do not believe that cybercrime will affect them at all or cause significant harm.

Prevention and use of protective measures, proper reporting, willingness to assist in collection of evidence, support to state policies in the area, public-private cooperation are examples where increased awareness of cybercrime would make a difference.

Supporting public awareness on cybercrime threats and responses should thus become a strategic priority.

Relevant authorities should consider the following actions:

- **Allocate more resources to increasing awareness of cybercrime threats and policies for the general public**. Authorities should consider more resources to target awareness of both the general population and private sector entities of threats, solutions and possibilities concerning cybercrime. It is understood that such investment is entirely reasonable in view of benefits of improved prevention, reporting and handling of cybercrime.

- **Adjust awareness action to the needs of most vulnerable groups.** Cyber Barometer Reports almost unanimously indicate children and elderly as two major groups that are most vulnerable to cyber threats and thus in need of increased awareness of potential threats and solutions. Another such group are smaller and medium enterprises whose operations depend on information technology systems, as they lack not only resources but also understanding to address current threats and potential solutions/prevention options.

- **Address cyberviolence as key area of concern for the general public**. The Cyber Barometer studies singled out online intimidation, threats and identity misuse as key threats that leave a long-lasting impact and are cause for major concern. Awareness actions and campaigns should address both criminal and other avenues to respond to cyberviolence, as supported by research and resources by the Council of Europe on the subject matter.[3]

- **Awareness activities should be varied and engaging.** It is rather important that cybercrime awareness campaigns do not simply restate the state policy goals or focus on limited set of activities, but are able to utilise social media and other forms of communication to effectively reach both the public at large as well as target vulnerable groups.

- **Partner with international donors, civil society and academia for improving general awareness.** While state resources may be scarce, partnerships with international donors, revising and including awareness into agreed assistance programmes, partnerships with universities, schools and other educational institutions, as well as engaging civil society especially on community/local levels – these are few examples of possibilities to maximise the reach and impact of awareness campaigns.

[3] https://www.coe.int/en/web/cyberviolence.

5. Strategic priority: Strengthening national training institutions

As – in addition to offences against and by means of computers – an increasing number of other offences involve evidence on computer systems or other storage devices, all law enforcement officers – from first responders to highly specialised computer forensic investigators – need to be enabled to deal with cybercrime and electronic evidence at their respective levels. Similarly, all judges and prosecutors need to be prepared to prosecute and adjudicate cybercrime and make use of electronic evidence in criminal proceedings.

Although much has been achieved in terms of training on cybercrime and electronic evidence in the region, with many law enforcement judicial training institutions now also teaching cybercrime and electronic evidence as part of in-service programmes, there is still much remaining toward the goal of fully sustainable, continuous education for all law enforcement and judicial authorities.

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.

Relevant authorities should consider the following actions:

- **Introduce cybercrime and electronic evidence training programmes at domestic training institutions where this has not been achieved.** Law enforcement agencies should have the skills and competencies necessary to investigate cybercrime, secure electronic evidence, carry out computer forensic analysis for criminal proceedings, and cooperate with other institutions (including cross-border). Similarly, judges and prosecutors should be able to handle electronic evidence in all criminal cases. Investment in such training is justified given the reliance of society on information technologies and associated risks.

- **Take ownership of the training materials and train trainers**. Numerous training concepts, programmes, guides and materials have already been developed by the Council of Europe.[4] This vast resource of training materials could be adapted to the needs of domestic training institutions with support of the capacity building programmes. Trainers should be trained in the delivery of the materials to ensure sustainability.

- **Introduce measures to ensure that law enforcement and judicial training on cybercrime and electronic evidence is compulsory.** It is important to recognise that electronic evidence impacts on all criminal activities and training in recognising and dealing with electronic evidence is needed by all criminal justice professionals and not only those in specialised units. Training institutions should integrate basic and advanced training modules on cybercrime and electronic evidence in their regular training curricula for initial and in-service training.

- **Consider the implementation of procedures to ensure best value for the investment in cybercrime training.** Cybercrime and computer forensics training is very expensive. In order to ensure that an adequate return is received for the investment, States should ensure that staff are appointed to and remain in posts that reflect the level of knowledge and skills they have. To this end, training and human resource strategies need to be complimentary.

[4] https://www.coe.int/en/web/octopus/training

6. Strategic priority: Financial investigations and prevention and control of fraud and money laundering on the Internet

Most crime involving the Internet and other information technologies is aimed at generating economic profit through different types of fraud and other forms of economic and serious crime. Large amounts of crime proceeds are thus generated and are circulating on the Internet. More recent technological advances in the use of virtual currencies and Darknet further exacerbate these challenges.

Therefore, financial investigations targeting the search, seizure and confiscation of crime proceeds and measures for the prevention of fraud and for the prevention and control of money laundering on the Internet should continue to be a strategic priority.

Governments should consider the following actions:

- **Establish an online platform for public reporting on fraud on the Internet and on cybercrime in general.** The use of standardised reporting templates will allow for a better analysis of threats and trends, of criminal operations and organisations, and of patterns of money flows and money laundering. This will facilitate measures by criminal justice authorities and financial intelligence units to prosecute offenders and to seize and confiscate crime proceeds. The platform should also serve preventive functions (public awareness and education, threat alerts, tools and advice). The more domestic platforms are harmonised with those of other States, the easier it will facilitate regional and international analyses and action.

- **Promote pro-active parallel financial investigations** when investigating cybercrime or offences involving information technologies/the Internet. This requires increased interagency cooperation between authorities responsible for cybercrime and for financial investigations as well as financial intelligence units. Joint training may facilitate such interagency cooperation.

- **Create trusted fora** (domestic and regional) for public/private information sharing on cyber threats regarding the financial sector. Domestic fora should be available to key stakeholders (such as financial sector representatives, Internet service providers, cybercrime units, financial intelligence units, Computer Security Incident Response Teams). Their purpose is to identify threats, trends, tools and solutions to protect the financial sector against cybercrime. The regional forum should consist of the fora established at domestic levels.

- **Establish the legal framework for the seizure and confiscation of crime proceeds** and digital assets as well as for the prevention of money laundering on the Internet. This should include digital assets, such as e-money and virtual currencies. Rules, regulations and procedures for anti-money laundering should also apply to Internet-based payment systems.

- **Exploit opportunities for more efficient international cooperation.** Linking anti-money laundering measures and financial investigations with cybercrime investigations and computer forensics offers added possibilities for international cooperation. Governments should make use of the opportunities available under the Budapest Convention on Cybercrime, the Convention on the Laundering, Search, Seizure and Confiscation of Proceeds from Crime and the Financing of Terrorism (CETS 198) of the Council of Europe and the revised 40 Recommendations of the Financial Action Task Force (FATF), as well as other standards and guidance from both international partners and capacity building programmes run by the Council of Europe.[5]

[5] https://www.coe.int/en/web/cybercrime/iproceeds-2

7. Strategic priority: Improving the efficiency of international and public/private co-operation

Cybercrime and electronic evidence are transnational by nature, thus requiring efficient international cooperation. Immediate action is required to secure electronic evidence in foreign jurisdictions and to obtain the disclosure of such evidence. However, the inefficiency of international cooperation, in particular of mutual legal assistance, is still considered among the main obstacles preventing effective action against cybercrime.

Similarly, cooperation between law enforcement agencies and service providers and other private sector entities is essential for protecting the rights of Internet users and for protecting them against crime. Effective investigations of cybercrime are often not possible without the cooperation of Service providers. However, such cooperation needs to take into account the different roles of law enforcement and of Service providers as well as the privacy rights of users.

Enhanced international cooperation on cybercrime and electronic evidence, supported by law enforcement/service provider cooperation and public/private sharing of information in line with data protection regulations, should become a strategic priority.

Governments should consider the following actions:

- **Utilise the possibilities of the Budapest Convention on Cybercrime and its Second Protocol to the widest extent possible**. Making full use of Articles 23 to 35 of the Budapest Convention, as well as new tools and possibilities of the Second Additional Protocol to the Convention, including legislative adjustments and improved procedures, is key to improving cross-border cooperation. Measures and training to accelerate mutual legal assistance should be implemented. Governments (Parties and Observers to the Convention) should actively participate in the work of the Cybercrime Convention Committee (T-CY) and should engage in cooperation with the specialised agencies and institutions of the European Union.

- **Strengthen the effectiveness of 24/7 points of contact.** Such contact points have been established in all States in line with Article 35 Budapest Convention, but their role needs to be further enhanced to be more pro-active and fully functional. Participation in annual meetings of the 24/7 Network, organised annually by the Cybercrime Programme Office of the Council of Europe, is key to ensuring coordination with partners and improvement of functioning of the Network.

- **Evaluate the effectiveness of international cooperation.** Ministries of Justice and of Interior and Prosecution Services should collect statistical data on international cooperation requests regarding cybercrime and electronic evidence, including the type of assistance requests, the timeliness of responses and the procedures used. This should help identify good practices and remove obstacles to cooperation. They may engage with regional partners in an analysis of the issues adversely affecting international cooperation.

- **Establish clear rules and procedures at the domestic level for law enforcement access to data** held by service providers and other private sector entities in line with data protection regulations. A clear legal basis in line with the procedural law provisions and the safeguards and conditions of the Budapest Convention on Cybercrime will help meet human rights and rule of law requirements. Various guidance and assessments by the Council of Europe,[6] including through its capacity building programmes in the region,[7] should be taken into account to address these needs.

[6] https://www.coe.int/en/web/cybercrime/all-reports.

[7] https://www.coe.int/en/web/cybercrime/cybereast-studies-and-reports.

- **Facilitate private/public information sharing across borders.** Private sector entities hold large amounts of data on cybersecurity incidents. The transborder sharing of such data would help improve the security of the information infrastructure as well as investigate offenders. Governments should consider legislation implementing the requirements and tools of the Second Protocol to the Budapest Convention on Cybercrime, including applicable safeguards.

- **Foster a culture of cooperation between law enforcement and service providers.** Memoranda of understanding between law enforcement and Internet Service Providers are a fundamental tool in this respect. Regional coordination of such MOUs would facilitate the ability of law enforcement authorities to conduct investigations across regional borders, with the knowledge that comparable standards have been adopted in other States. MOUs combined with clear rules and procedures may also facilitate the cooperation with multi-national Service providers and other private sector entities including in the disclosure of data stored in foreign jurisdiction or on cloud servers that are managed by these Service providers.

8. Strategic priority: Coordinated responses to cyber threats through cooperation between cybersecurity experts and law enforcement

In the landscape of growing threats of cybercrime, further exacerbated by security risks and political challenges in the Eastern Partnership region, the Computer Security Incident Response Teams (CSIRTs) play an increasingly important role in cooperation with law enforcement to deter and respond to cybersecurity incidents and cybercrime. In addition to providing threat intelligence, CSIRTs invest significant efforts into prevention of cyber-attacks, perform damage mitigation, assist law enforcement in advanced forensics of attacks and coordinate technical responses at a national level, especially where cyberattacks target critical infrastructure.

It is therefore expected that CSIRTs and criminal justice authorities should have in place effective collaboration frameworks, where roles, responsibilities and segregation of duties are defined and agreed upon.

Coordinated response to cyber threats through cooperation between CSIRTs and law enforcement should thus become a strategic priority.

Governments should consider the following actions:

- **Implement agreed Standard Operating Procedures (SOPs) and the principles of cooperation,** agreed under the joint action of CyberEast and CyberSecurity EAST projects in the region’s countries. The SOP documents represent important national milestones for enhancing cooperation between cybersecurity and cybercrime professionals in all aspects, from initial incident reporting to joint capacity building. Implementation of these principles could be supported through joint capacity building programmes.

- **Establish common taxonomy and classifications for cybersecurity incidents and cybercrime reports, improving quality of reporting and coordination of response**. Special consideration should be given to single points of contact facilitating effective exchange and coordination between agencies, including organisation of joint operative meetings for intelligence and knowledge exchange.

- **Improve cybercrime and cybersecurity legislation to secure preservation and production of electronic evidence,** including in particular assistance in handling cyber-attacks and forensic expertise in cases requiring specialised skills of CSIRTs for supporting law enforcement in cybercrime investigations, (malware analysis, network investigations, threat intelligence and others) as well as elaborate the respective legal and regulatory framework aimed at coherent transposition of computer incident artefacts into cybercrime case investigations in a forensically sound manner.

- **Hold regular joint training, exercise and professional exchange between CSIRTs and cybercrime units as well as set-up and operation of JITs** to improve communication methods, promote use of common templates for sharing information, increase expertise in handling and securing e-evidence, and improve the protection of critical information infrastructure and the quality of investigations on incidents occurred therein.