CyberCrime@EAP

EU/COE Eastern Partnership – Council of Europe Facility: Cooperation against Cybercrime

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

Data Protection and Cybercrime Division
Council of Europe
Kyiv, Ukraine, 31 October 2013

www.coe.int/cybercrime

Funded by the European Union

EUROPEAN UNION

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Contents

Note: This document has been developed with the support of the CyberCrime@EAP joint project of the European Union and the Council of Europe on cooperation against cybercrime under the Eastern Partnership Facility.

Contact

For further information please contact:

Data Protection and Cybercrime Division
Directorate General of Human Rights and Rule of Law
Council of Europe
Strasbourg, France
Tel +33-3-9021-4506
Fax +33-3-9021-5650
Email alexander.seger@coe.int

Disclaimer

This document does not necessarily reflect official positions of the Council of Europe, the European Union or of the parties to the instruments referred to.

Declaration on Strategic Priorities for Cooperation against Cybercrime

We, representatives of Ministries of Interior and Security,
Ministries of Justice and Offices of Prosecutor's General
of States participating in the CyberCrime@EAP project of the
Eastern Partnership Facility

- Meeting at this regional Conference on Strategic Priorities on Cybercrime held in Kyiv, from 30 to 31 October 2013, in cooperation with the Council of Europe and the European Union;

- Taking note of the Joint Declaration on Eastern Partnership Justice and Home Affairs adopted by Ministers responsible for justice and home affairs of European Union Member States and States participating in the Eastern Partnership (Luxembourg, 8 October 2013) which stresses, *inter alia*, the importance of enhancing cooperation against cybercrime through effective application of the standards of the Budapest Convention on Cybercrime;

- 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, including in particular children;

- 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 as a guideline for domestic legislation and a framework for international cooperation;

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

- Considering, in particular, that partnerships should be sought between the European Cybercrime Centre (EC3) at Europol and our law enforcement authorities;

- Grateful for the support provided by the European Union and the Council of Europe through the CyberCrime@EAP regional project;

- 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 strategic priorities for cooperation against cybercrime

presented at this conference

and

we are committed to

- Pursue 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 that meets human rights and rule of law requirements;

- Strengthen specialised law enforcement units and the specialisation of prosecution services with respect to cybercrime and electronic evidence;

- Implement sustainable law enforcement training strategies;

- Support the training of judges and prosecutors on cybercrime and electronic evidence;

- Pursue comprehensive strategies to protect children against online sexual exploitation and sexual abuse in line with the Lanzarote Convention;

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

- Strengthen cooperation with the private sector, in particular between law enforcement authorities and Internet service providers;

- Engage in efficient regional and international cooperation;

- 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

Kyiv, Ukraine, 31 October 2013

Appendix: Strategic priorities for cooperation against cybercrime

1. Strategic priority: 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 adoption of cybersecurity strategies by many 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.

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:

- **Pursue cybercrime policies or strategies** with the objective of ensuring an effective criminal justice response to offences against and by means of computers as well as to any offence involving electronic evidence. Consider as elements of such policies or strategies preventive measures, legislation, specialised law enforcement units and prosecution services, interagency cooperation, law enforcement and judicial training, public/private cooperation, effective international cooperation, financial investigations and the prevention of fraud and money laundering, and the protection of children against sexual violence.

- Ensure that human rights and rule of law requirements are met when taking measures against cybercrime.

- **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.

- Create awareness and promote preventive measures at all levels.

- **Engage in public/private cooperation**, including in particular in the cooperation between law enforcement authorities and Internet Service Providers.

- **Engage in international cooperation to the widest extent possible.** This includes making full use of the existing bi- and multilateral and regional agreements, in particular the Budapest Convention on Cybercrime. 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 European Cybercrime Centre (EC3) and other initiatives of the European Union.

- **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: A complete and effective legal basis for criminal justice action

Adequate legislation is the basis for criminal justice measures on cybercrime and the use of electronic evidence in criminal proceedings. States participating in the CyberCrime@EAP project 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.[1] 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.

The adoption of complete and effective legislation that meets human rights and rule of law requirements should be 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 (follow up to assessment by Cybercrime Convention Committee), but also other rules on access to data held by private sector entities.

- **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.

- **Ensure that law enforcement powers are subject to conditions and safeguards in line with Article 15 Budapest Convention.** This should include judicial oversight of intrusive powers but also respect of principles of proportionality and necessity.

- **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.

[1] 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).

3. Strategic priority: Specialised cybercrime units

Cybercrime and electronic evidence require a specialised response by criminal justice authorities. Law enforcement authorities and prosecution services need to be able to investigate and prosecute offences against computer data and systems, offences by means of computers as well as electronic evidence in relation to any crime. In all States participating in the CyberCrime@EAP project, the creation or strengthening of police-type cybercrime units is in progress and the specialisation of prosecutors is under consideration in some. This process should be pursued. It is essential to understand that technology changes day by day and that the workload of cybercrime and forensic units is increasing constantly. The resourcing (staff, equipment, software) and maintenance of specialised skills and the adaptation of such units to emerging requirements is a continued challenge.

The continued strengthening of specialised cybercrime units should be strategic priority.

Relevant authorities should consider the following actions:

- **Establish – where this has not yet been done – specialised cybercrime units within the criminal police.** The exact set up and functions should be the result of a careful analysis of needs and be based on law.

- **Enhance the specialisation of prosecutors.** Consider the establishment of specialised prosecution units or, alternatively, of a group of specialised prosecutors to guide or assist other prosecutors in cases involving cybercrime and electronic evidence.

- **Review the functions and resourcing of specialised units on a regular basis.** This should allow to adjustments and thus to meet new challenges and increasing demands.

- Facilitate cooperation and exchange of good practices between specialised units at regional and international levels.

- **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. Consider making use of the Guide on Electronic Evidence developed under the CyberCrime@IPA project in cooperation with experts of the Eastern Partnership region.

4. Strategic priority: Law enforcement training

Law enforcement authorities need to be able not only to investigate offences against and by means of computer systems but also deal with electronic evidence in relation to any type of crime. With the exponential growth in the use of information technologies by society, law enforcement challenges have increased equally. 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. Elements of law enforcement training strategies have been identified, but consistent training strategies have not yet been adopted.

The preparation and implementation of sustainable training strategies to train law enforcement officers at the appropriate level should be a strategic priority.

Relevant authorities should consider the following actions:

- **Implementation of a domestic law enforcement training strategy.** The objective should be to ensure that law enforcement agencies have the skills and competencies necessary to investigate cybercrime, secure electronic evidence, carry out computer forensic analysis for criminal proceedings, assist other agencies and contribute to network security. Investment in such training is justified given the reliance of society on information technologies and associated risks.

- **Include rules and protocols on the handling of electronic evidence in all levels of national training.** 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 law enforcement operatives and not only those in specialised units. This training could be based on the Guide on Electronic Evidence developed under the CyberCrime@IPA project.

- **Consider the introduction of individual training plans for specialist investigators.** The changes in technology and the manner in which criminal abuse that technology mean that there is a need for an appropriate number of highly trained personnel that are competent and able to conduct investigations and or digital evidence examinations at the highest level. It will also enhance their status within the criminal justice system.

- **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.

5. Strategic priority: Judicial training

As – in addition to offences against and by means of computers – an increasing number of other types of offences involve evidence on computer systems or other storage devices, eventually all judges and prosecutors need to be prepared to deal with electronic evidence. A clear need for systematic and sustainable training for judges and prosecutors has been identified in all States participating in the CyberCrime@EAP project.

Enabling all judges and prosecutors to prosecute and adjudicate cybercrime and make use of electronic evidence in criminal proceedings should remain a strategic priority.

Relevant authorities should consider the following actions:

- **Adapt existing training materials and train trainers**. Training concepts and materials have already been developed by the Council of Europe and could be adapted to the needs of domestic training institutions. Trainers should be trained in the delivery of the materials.

- **Mainstream judicial training on cybercrime and electronic evidence.** Domestic institutions for the training of judges and prosecutors should integrate basic and advanced training modules on cybercrime and electronic evidence in their regular training curricula for initial and in-service training.

- **Introduce measures to ensure that judicial training on cybercrime and electronic evidence is compulsory.** It has been apparent during the project that training for judges and prosecutors is voluntary in most project areas. This led to many instances where participants only attended training for very short periods of courses and did not benefit fully from the training that was delivered.

- **Introduce training records for individual judges and prosecutors.** In order to ensure that best use is made of the training delivered to judges and prosecutors, it is advisable that a record is kept of all training received by individuals so as to inform requirements for further specialised training and to ensure the right people are trained and their skills utilised appropriately.

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.

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 become 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). Consideration should furthermore be given to the findings of the MONEYVAL typology study on criminal money flows on the Internet of March 2012.[2]

[2] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/MONEYVAL_2012_6_Reptyp_flows_en.pdf

7. Strategic priority: Cooperation between law enforcement and Internet service providers

Cooperation between law enforcement agencies and Internet service providers (ISPs) 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 ISPs. However, such cooperation needs to take into account the different roles of law enforcement and of ISPs as well as the privacy rights of users.

Enhanced law enforcement/ISP cooperation and public/private sharing of information in line with data protection regulations should become a strategic priority.

Governments should consider the following actions:

- **Establish clear rules and procedures at the domestic level for law enforcement access to data** held by ISPs 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. Guidelines[3] adopted at the Octopus Conference of the Council of Europe in 2008 may help law enforcement and ISPs organise and structure their cooperation. Governments should facilitate the use of the expedited preservation provisions (Articles 16, 17, 29 and 30) of the Budapest Convention taking into account the results of the assessments by the Cybercrime Convention Committee.[4]

- **Foster a culture of cooperation between law enforcement and ISPs.** 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 ISPs and other private sector entities including in the disclosure of data stored in foreign jurisdiction or on cloud servers that are managed by these ISPs.

- **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 and the conclusion of agreements allowing for private/public information sharing and encourage the development of guidelines to facilitate the sharing of information intra- and transborder, including procedural, technical, legal and data protection safeguards.

[3] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/LEA_ISP/default_en.asp.
[4] Assessment report adopted by the T-CY in December 2012 http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/TCY2013/TCYreports/TCY_2012_10_Assess_report_v30_public.pdf

8. Strategic priority: More efficient regional and international cooperation

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.

Rendering international cooperation on cybercrime and electronic evidence more efficient should be a strategic priority.

Governments should consider the following actions:

- **Exploit the possibilities of the Budapest Convention on Cybercrime and other bilateral, regional and international agreements on cooperation in criminal matters**. This includes making full use of Articles 23 to 35 of the Budapest Convention in relation to police-to-police and judicial cooperation, including legislative adjustments and improved procedures. Governments (parties and observers to the Convention) should fully participate in the 2013 assessment of the international cooperation provisions of the Budapest Convention that is being undertaken by the Cybercrime Convention Committee (T-CY) and any follow up resulting from this assessment. They should follow up to the T-CY assessment of 2012 and promote the use of Articles 29 and 30 of the Budapest Convention regarding international preservation requests.

- **Provide for training and sharing of good practices.** Authorities for police and judicial cooperation should engage in domestic, regional and international training and the sharing of good practices. This should facilitate cooperation based on trust.

- **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.

- **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 enhanced and they may need to become more pro-active and fully functional.

- **Compile statistics on and review the effectiveness of 24/7 contact points** and other forms of international cooperation on a regular basis.