GLACY
Global Action on Cybercrime
Action globale sur la cybercriminalité

Bucharest, 28 October 2016

Strategic priorities for cooperation on cybercrime and electronic evidence in GLACY countries

Adopted at the closing conference of the
GLACY project on Global Action on Cybercrime
Bucharest, 26-28 October 2016

www.coe.int/cybercrime

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Contents

Declaration on Strategic Priorities for Cooperation on Cybercrime 3

Appendix: Strategic priorities for cooperation on cybercrime 5

1. Strategic priority: Mainstreaming cybercrime and electronic evidence in the criminal justice system 5
2. Strategic priority: Continuous law reform and development 6
3. Strategic priority: Strengthening institutional capacities on cybercrime and electronic evidence 7
4. Strategic priority: Law enforcement training 8
5. Strategic priority: Judicial training 9
6. Strategic priority: Cooperation between law enforcement and service providers 10
7. Strategic priority: More efficient regional and international cooperation 11

Contact

Cybercrime Programme Office of the Council of Europe (C-PROC)
Tel +33-3-9021-4506
Email alexander.seger@coe.int

Declaration on Strategic Priorities for Cooperation on Cybercrime

We, representatives of Mauritius, Morocco, Philippines, Senegal, South Africa, Sri Lanka and Tonga participating in the Global Action on Cybercrime (GLACY)

- Meeting at the Closing Conference of GLACY Project in Bucharest, Romania on 28 October 2016;

- Underlining the value of the Budapest Convention on Cybercrime as a guideline for domestic legislation and a framework for international cooperation on cybercrime and electronic evidence;

- 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;

- Conscious of the value of the Protocol to the Budapest Convention on Cybercrime regarding Xenophobia and Racism for countering hate speech contributing to radicalisation and violent extremism;

- Aware that any crime may involve electronic evidence on computer systems and that lawful access to such evidence is essential to ensure the rule of law and to protect human rights;

- Recognising the positive obligation of governments to protect individuals against cybercrime and other offences involving electronic evidence;

- Mindful of the need to respect fundamental rights and freedoms, including the protection of individuals with regards 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 on cybercrime and electronic evidence require efficient regional and international cooperation;

- Grateful for the support provided by the European Union and the Council of Europe through the project on Global Action on Cybercrime (GLACY);

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

We endorse

the strategic priorities for cooperation on 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 comprehensive 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 on the handling of electronic evidence in relation to any crime;
- Pursue comprehensive strategies to protect children against online sexual exploitation and sexual abuse;
- Strengthen cooperation with the private sector, in particular between law enforcement authorities and Internet and/or other communication service providers;
- Engage in efficient regional and international cooperation;
- Share experience with other regions of the world to support capacity building against cybercrime;
- Promote awareness of the Budapest Convention on Cybercrime at the global level.

Declaration adopted by acclamation in

Bucharest, Romania, 28 October 2016

Appendix: Strategic priorities for cooperation on cybercrime

1. Strategic priority: Mainstreaming cybercrime and electronic evidence in the criminal justice system

As societies are transformed by information and communication technology, the security of ICT has become a policy priority of many governments, having in mind the positive obligation to protect people and their rights against cybercrime and to bring offenders to justice. Prevalence of cybercrime and the increasing reliance on electronic evidence for the investigation and prosecution of traditional forms of crime thus necessitate the response to cybercrime challenges on the same level as to other forms of crime that undermine state security, economic stability, or wellbeing of individuals and society.

In this light, relevant authorities may consider the following actions:

- **Pursue cybercrime and cybersecurity 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.

- **Create awareness of the challenges of cybercrime and electronic evidence and promote preventive measures** at all levels. This includes raising awareness of electronic evidence as a transversal challenge among decision-makers in governments and among members or parliaments.

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

- **Establish online platforms for public reporting on cybercrime** or integrate cybercrime reporting into already existing reporting platforms and solutions. 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.

- **Engage in public/private cooperation**, including in particular in the cooperation between law enforcement authorities and 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. Actively participate in the work of the Cybercrime Convention Committee (T-CY).

- **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: Continuous law reform and development

Adequate legislation is the basis for criminal justice measures on cybercrime and the use of electronic evidence in criminal proceedings. States participating in the GLACY project have made much progress in bringing their legislation in line with the Budapest Convention; however, much work remains to be done to ensure continuous development of legislation in response to new threats and challenges in cyberspace, and to implement relevant standards and safeguards, such as globally recognized standards on data protection, regulations on the protection of children against sexual violence, or actions against crime proceeds and money laundering.

The adoption and continuous review and update of effective legislation that meets human rights and rule of law requirements should be a strategic priority.

Relevant authorities should consider the following actions:

- **Adopt and/or improve procedural law provisions to secure electronic evidence by law enforcement**. This should include in particular domestic legal provisions and implementing regulations on production orders (Article 18) and on the expedited preservation of data (Articles 16, 17, 29 and 30) as foreseen under the Budapest Convention in order to ensure lawful 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 of the 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 Convention for the protection of individuals with regard to automatic processing of personal data (ETS 108) or other recognized and applicable standards.

- **Complete legislation and take preventive and protective measures on the protection of children against online sexual violence**, in line with the provisions of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention).

- Consider legislation in line with and accession to the **Additional Protocol to the Budapest Convention on Xenophobia and Racism** committed through Computer Systems.

- **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, both primary and sector-specific, should in particular allow for swift domestic and international information exchange.

3. Strategic priority: Strengthening institutional capacities on cybercrime and electronic evidence

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. 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, and software) and maintenance of specialised skills and the adaptation of such units to emerging requirements is a continued challenge.

Strengthening of specialised cybercrime units and capacities to deal with electronic evidence in criminal cases should be a 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. 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.

- **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.

- **Ensure the setup, training and continuous capacity building of digital forensics capabilities** either within specialised investigative units on cybercrime or other relevant authorities.

- **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, including standards and guides developed by the Council of Europe and other relevant documents.

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.

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 at 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.

- **Consider the introduction of individual training plans for specialist investigators.** The changes in technology and the manner in which criminals abuses from that technology means 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 costly. 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

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, which means that eventually all judges and prosecutors need to be prepared to deal with electronic evidence. There is a clear need for systematic and sustainable training for judges and prosecutors on cybercrime and electronic evidence.

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:

- **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.

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

- **Provide judges with reference materials that will be of assistance on the bench when adjudicating cybercrime matters.** In order to integrate cybercrime knowledge a bench book should be developed to expedite the handling of matters related to cybercrime and electronic evidence.

- **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: Cooperation between law enforcement and service providers

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 and other offences involving electronic evidence 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 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:

- **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. Guidelines adopted at the Octopus Conference of the Council of Europe in 2008 may help law enforcement and service providers to 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 and ensure full implementation of Article 18 on production orders.

- **Foster a culture of cooperation between law enforcement and service providers as well as other private sector entities**. Memoranda of understanding between law enforcement and private sector entities 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 included in the disclosure of data stored in foreign jurisdiction or on cloud servers that are managed by these service providers.

- **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.

7. 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 a major obstacle preventing effective action on 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 promote the use of Articles 29 and 30 of the Budapest Convention regarding international preservation requests.

- **Establish 24/7 points of contact under Article 35 Budapest Convention and strengthen their effectiveness** through adequate resourcing, training, legal powers and support to pro-active cooperation at domestic levels and with foreign counterparts.

- **Allocate more and technology-literate staff and other resources for mutual legal assistance** not only at central levels but also at the level of institutions responsible for executing requests, including prosecution services.

- **Establish emergency procedures** for access to and disclosure of data in situations related to risks of life and similar exigent circumstances.

- **Make use of electronic transmission of requests** in line with Article 25.3 Budapest Convention on expedited means of communication.

- **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.