



Global Project on Cybercrime

Capacity building on cybercrime

Discussion paper

Version 1 November 2013
Data Protection and Cybercrime Division,
Council of Europe, Strasbourg

www.coe.int/cybercrime

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Abstract

The international community has reached broad agreement, at political levels, on capacity building as an effective way to address the threat of cybercrime and the challenges related to electronic evidence. The purpose of this discussion paper is to illustrate how such a political agreement can be translated into actual capacity building programmes. It offers pointers, arguments and resources for organisations prepared to provide support, for those requiring assistance and for those designing cooperation projects. Capacity building on cybercrime and electronic evidence is not only aimed at strengthening the rule of law and human rights in cyberspace and at enhancing cybersecurity but also at contributing to human development, poverty reduction and democratic governance. This discussion paper may encourage, therefore, a stronger role of development cooperation organisations in capacity building on cybercrime.

This version represents work in progress.

Comments should be sent to alexander.seger@coe.int

CONTACT

Data Protection and Cybercrime Division
Directorate General of Human Rights and Rule of Law
Council of Europe, F-67075 Strasbourg Cedex
France

Tel +33 3 9021 4506
Fax +33 3 8841 3955
Email alexander.seger@coe.int

DISCLAIMER

The views expressed in this technical report do not necessarily reflect official positions of the Council of Europe, of the donors funding this project or of the Parties to the treaties referred to.

Contents

1	Cybercrime – a case for capacity building.....	4
2	The concept of cybercrime	6
2.1	About cybercrime.....	6
2.2	The question of electronic evidence	6
2.3	Cybercrime and cybersecurity.....	7
2.4	Cybercrime in the South	7
3	Justifying capacity building programmes	10
4	Objectives of capacity building programmes	12
4.1	Rationale and objectives	12
4.2	Supporting a process of change	13
5	Elements of capacity building programmes.....	14
5.1	Cybercrime policies and strategies.....	14
5.2	Legislation	15
5.3	Cybercrime reporting	15
5.4	Prevention	16
5.5	Specialised units.....	16
5.6	Law enforcement training.....	17
5.7	Judicial training	17
5.8	Public/private cooperation.....	18
5.9	International cooperation.....	18
5.10	Protection of children	19
5.11	Financial investigations and prevention of fraud and money laundering.....	19
5.12	Prevention and control of terrorist use of ICT	20
6	Sequencing	21
7	Capacity building: the experience of the Council of Europe	22
7.1	Overview	22
7.2	Projects.....	23
7.3	C-PROC: Cybercrime Programme Office of the Council of Europe.....	27
8	Conclusions	28

1 Cybercrime – a case for capacity building

People all over the world depend on technology to communicate, access, share and produce information, organise themselves, participate in public life, hold authorities accountable, enjoy their rights and benefit from economic opportunities. It is clear that Information and communication technologies (ICT) over the past two decades not only contributed to a transformation of societies in the North but also in the South “where technological adaptation ... led to new kinds of innovation with immediate human development benefits”¹. ICT “enlarge people’s choices” and can be considered a “powerful tool for human development and poverty reduction”.²

At the same time, the reliance of ICT makes societies vulnerable to threats such as cybercrime, that is, offences against computer systems and offences committed by means of computer systems. Cybercrime affects the security and rights of individuals, it strengthens transnational criminal organisations, it puts at risk the critical infrastructure on which societies depend and it undermines the security, trust and confidence that are necessary to reap the benefits of ICT.

Meeting the challenge of cybercrime requires a set of measures that involve a wide range of stakeholders, from individual computer users, to private sector entities, non-governmental organisations, governments and international organisations and initiatives. Cybercrime is crime. Given the positive obligation of governments to protect society and individuals against crime, an effective criminal justice response is particularly necessary.

The international community has been reflecting for more than 25 years on how best to address the threat of cybercrime at the international level as a matter of crime prevention and criminal justice. This resulted, among other things, in the adoption of the Budapest Convention on Cybercrime in 2001 which serves many countries around the world as a guideline and, for those that are parties, as a framework for international cooperation.³

Recent years have shown that cyberspace and related security questions have become that important – a matters of “national interest” for many governments – that positions are highly “diverse” and binding agreements that go further than existing treaties are difficult to achieve.

However, there is one approach that receives broad international support, namely to address cybercrime through capacity building.⁴

¹ UNDP (2013): Human Development Report 2013 – The Rise of the South: Human Progress in a Diverse World. New York. http://hdr.undp.org/en/media/HDR_2013_EN_complete.pdf

² UNDP (2001): Human Development Report 2001 – Making new technologies work for human development. New York. <http://hdr.undp.org/en/media/completenew1.pdf>

³ www.coe.int/cybercrime

⁴ http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_3_E.pdf

See also Resolution 22/8 adopted at by United Nations Commission for Crime Prevention and Criminal Justice in April 2013 <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/V13/835/69/PDF/V1383569.pdf?OpenElement>

Capacity building as an approach on cybercrime has a number of advantages:

- Responding to needs and producing impact. Two-thirds or more of United Nations Member States have either adopted legislation related to cybercrime already, or are engaged in a process of legislative reform, but still require the criminal justice capacities necessary to enforce laws and engage in international cooperation. Capacity building responds to needs such as advice on legislation and enabling criminal justice practitioners to apply laws in practice. Capacity building programmes are thus likely to be of immediate benefit and to produce tangible results ranging from stronger legislation to specialized cybercrime units, skills for law enforcement, prosecutors and judges, increased investigation, prosecution and adjudication of cybercrime and other offences involving electronic evidence, or improved public/private, interagency and international cooperation.
- Multi-stakeholder cooperation. Capacity building on cybercrime is not about governments only but requires the cooperation of multiple stakeholders, including private sector entities, civil society or academia but also different international organisations and initiatives. In short, it implies the type of multi-stakeholder cooperation that characterizes the current approach to Internet governance.
- Cybercrime and the development agenda. Capacity building programmes on cybercrime can be linked to other technical cooperation programmes aimed at human development and democratic governance and to the development agenda of governments, donors and international organisations.
- Reducing the digital divide. Cybercrime and electronic evidence are challenges for criminal justice authorities in all regions of the world. However, many countries in the South seem particularly vulnerable. Capacity building – including resource mobilization, networking, sharing of good practices and confidence building – enables stronger participation of the South in international efforts on cybercrime.
- Broad international support. As indicated, the international community has been consistently expressing its support to capacity building on cybercrime. Technical cooperation programmes, therefore, can commence without delay. In fact, capacity building may help overcome political divisions.

The purpose of this paper is to illustrate how agreements on capacity building reached internationally at political levels can be translated into actual cooperation programmes.

“Capacity building” is understood here as enabling criminal justice authorities to meet the challenge of cybercrime and electronic evidence. This entails strengthening the knowledge and skills and enhancing the performance of criminal justice organisations including their cooperation with other stakeholders. It should be aimed at protecting individuals and society against crime and at protecting the rights of individuals, at promoting security, confidence and trust in ICT, at strengthening human rights, democracy and the rule of law in cyberspace and at contributing to human development.

The present paper will largely rely on the experience gained by the Council of Europe in recent years.

2 The concept of cybercrime

2.1 About cybercrime

Cybercrime is a complex and ever evolving threat of staggering proportions targeting every day millions of individuals, businesses, civil society and public sector organisations and costing hundreds of billions of Euros in damage.⁵

The concept of cybercrime⁶ comprises:

- offences against the confidentiality, integrity and availability of computer data and systems, that is, offences against computers, including also smart phones, tablets and other devices. These cover illegal access (such as “hacking” or computer espionage), the illegal interception of the transmission of computer data, data interference (the damaging, deletion, deterioration, alteration or suppression of computer data), system interference (the hindering of the functioning of computer systems, including denial of service attacks, “hacktivism” and attacks against critical information infrastructure through botnets) or the misuse of devices (the production, sale, procurement or otherwise making available of devices or data for the purpose of committing the above offences, such as “hacking” tools);
- offences committed by means of computer systems. This includes “old” forms of crime that obtain a new quality through the use of computers, such as computer-related forgery, computer-related fraud, child pornography and other forms of online sexual violence against children, or offences related to infringements of copyright and related rights on a commercial scale.

Most cases of cybercrime are likely to involve a combination of these types of conduct.

2.2 The question of electronic evidence

Beyond cybercrime (offences against or by means of computers), any crime may entail electronic evidence on a laptop, smart phone, tablet, server or any other type of computer or storage device. Examples may include location data proving that a suspected offender was indeed on the crime scene, an email requesting ransom for a kidnapped person, traffic data in a corruption case proving that two persons communicated with each other, communications proving membership in a criminal organisation, etc. While this is not “cybercrime” electronic evidence nevertheless brings major challenges for criminal justice authorities.

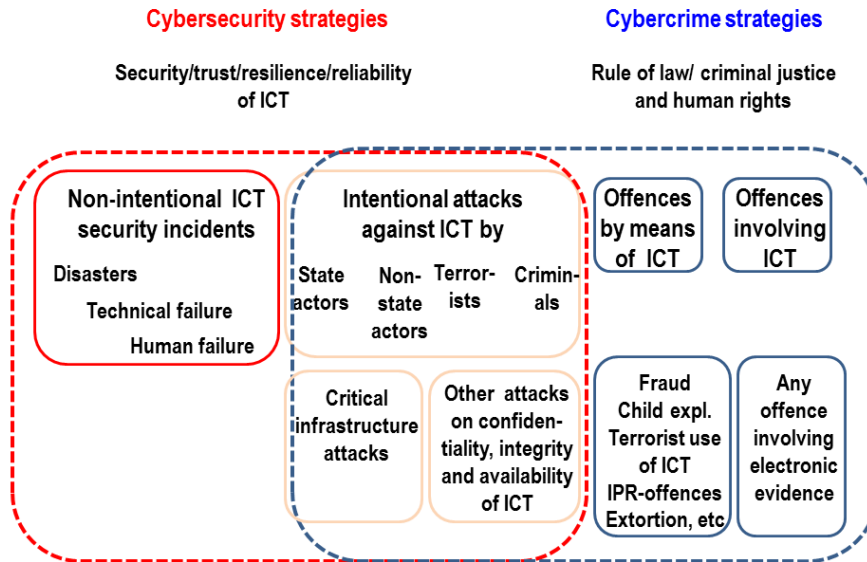
Cybercrime is thus not only a specific form of crime, but also – in particular when considering the question of electronic evidence – a horizontal issue and can be an element in almost any type of crime.

⁵For examples of threat reports, see: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf
<http://www.securelist.com/en/analysis/204792255/>
<http://www.microsoft.com/security/sir/default.aspx>
<http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf>

⁶ This concept is based on the logic of the Budapest Convention on Cybercrime (www.coe.int/cybercrime). See also the Guidance Notes of the Cybercrime Convention Committee on how this concept applies to new forms of cybercrime. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/Default_TCY_en.asp

2.3 Cybercrime and cybersecurity

The prevention and control of cybercrime and measures to enhance cybersecurity are mutually reinforcing. Cybersecurity is about the protection of the confidentiality, integrity and availability of computer data and systems in order to enhance security, resilience, reliability and trust in ICT. This includes technical, procedural and institutional measures for the protection against, mitigation of and recovery from intentional attacks and non-intentional incidents affecting in particular critical information infrastructure. An effective criminal justice response to offences against ICT thus reinforces cybersecurity.⁷



2.4 Cybercrime in the South

Cybercrime and the information society form an ecosystem. Crime is not only shaped by its political, economic, socio-cultural, technological, ecological and legal or regulatory environment, but adapts, interacts with and influences its environment. As individuals, businesses, the financial sector, and public services and infrastructures become highly dependent on ICT, criminals search and exploit vulnerabilities or morph and adapt to countermeasures in an opportunistic manner. Thus, increasing broadband penetration and ICT use with a weak regulatory and governance framework to protect computers, allows cybercrime to proliferate and undermine the human development potential of ICT in the South. Reports suggest, for example, that:

- malware infection rates are considerably higher in most countries of the South.⁸ Many exploits appear to be targeting vulnerabilities in computer systems located in the South;
- in Africa, as in other regions, criminals increasingly turn infected computers into externally controlled zombies for botnet activity;
- the ratio of websites distributing malware seems to be highest in some countries of Latin America, East and South-east Asia as well as Eastern Europe;

⁷ On the distinction between cybersecurity and cybercrime prevention and control see http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_cy_strats_rep_V23_30march12.pdf

⁸ <http://www.microsoft.com/security/sir/default.aspx>
<http://www.securelist.com/en/analysis/204792255/>

- the same is reported for the ratio of phishing sites – that is, fake or compromised websites aimed at stealing personal information for fraudulent purposes;
- different types of Internet fraud are widespread in the South. Advance-fee fraud schemes – such as “419 fraud”⁹ are operated by criminal enterprises associated with West Africa – cause major losses around the world;
- mobile payment services – via mobile or smart phones, tablets and similar – are becoming popular in Africa and other regions. However, a sizeable share of users of mobile payment services in Africa are reported to fall victim to cybercrime;
- criminal enterprises exploit the opportunities offered by the Internet, namely to trade in counterfeit medicines online. This is a very large criminal market. Countries in the South are the primary targets of substandard, non-approved or counterfeit medicines;
- many countries in the South are not able to protect their critical information infrastructure against intentional attacks or non-intentional security incidents.

Governments have the positive obligation to protect individuals against crime, including through criminal justice measures.

However, coercive law enforcement measures, such as the search and seizure of computer data or systems, or the interception of communications, represent interference in the rights of individuals. Therefore, they must:

- be prescribed by law and the law must be precise, clear, accessible and foreseeable;
- pursue a legitimate aim;
- be necessary, that is, it must respond to a pressing social need in a democratic society and thus be proportionate;
- allow for effective remedies;
- be subject to guarantees against abuse.¹⁰

⁹ Named after Article 419 of the Criminal Code of Nigeria which criminalises such conduct,

¹⁰ In the Budapest Convention on Cybercrime, conditions and safeguards limiting law enforcement powers are defined in Article 15. See:

[Article 15 Conditions and safeguards under the Budapest Convention on Cybercrime](#)
[Internet: case law of the European Court of Human Rights](#)

ICT, human rights and human development: References

In 2003, the World Summit on the Information Society agreed on a people-centred and development-oriented perspective on ICT:

“ 1. We, the representatives of the peoples of the world, assembled in Geneva from 10-12 December 2003 for the first phase of the World Summit on the Information Society, declare our common desire and commitment to build a people-centred, inclusive and development-oriented Information Society, where everyone can create, access, utilize and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life, premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights.”¹¹

A decade later, it seems clear that ICT not only contributed to a transformation of societies in the North but also in the South “where technological adaptation ... led to new kinds of innovation with immediate human development benefits”. According to the United Nations Development Programme:

“Cellular banking is cheaper and easier than opening a traditional bank account, farmers can obtain weather reports and check grain prices and entrepreneurs can provide business services through mobile phone kiosks. These and other transformations multiply the possibilities of what people can do with technology: participating in decisions that affect their lives; gaining quick and low-cost access to information; producing cheaper, often generic medicines, better seeds and new crop varieties; and generating new employment and export opportunities. These new technologies are connecting people in formerly isolated and marginalized rural communities and in poor urban neighbourhoods. They also give them access to valuable tools, resources and information and enable them to more actively participate in the wider national and even global society.”¹²

However, the WSIS also underlined:

“Building confidence and security in the use of ICT” is a prerequisite for societies to fully benefit from such technologies: “It is necessary to prevent the use of information resources and technologies for criminal and terrorist purposes, while respecting human rights.”¹³

¹¹ <http://www.itu.int/wsis/docs/geneva/official/dop.html>

¹² UNDP (2013): Human Development Report 2013 – The Rise of the South: Human Progress in a Diverse World. New York. http://hdr.undp.org/en/media/HDR_2013_EN_complete.pdf

¹³ Principle 36. <http://www.itu.int/wsis/docs/geneva/official/dop.html>

3 Justifying capacity building programmes

Capacity building programmes require resources. A substantiated justification is necessary to explain why precious resources should be allocated to programmes on cybercrime and not to other sectors where needs may appear to be more pressing. Obviously, each project or programme will have its own specific justification. At a high level, reasons to allocate resources to programmes on cybercrime include the following:

- The reliance of societies on ICT. The fact that societies increasingly rely on ICT is true for all regions of the world which have experienced major growth in Internet usage¹⁴, increased availability of broad band and increasing use of mobile phones and related applications.¹⁵ Apart from individual usage, public services and the public and private sector infrastructure as a whole are dependent on ICT. Ensuring security of and confidence and trust in ICT should, therefore, be a priority of any government, and this should also be reflected in development cooperation activities aimed at the strengthening of capacities on cybercrime and electronic evidence.
- The threat of cybercrime and the challenge of electronic evidence. Offences against and by means of computers are not peripheral phenomena anymore. The more societies make use of ICT and related services, the more are criminals exploiting vulnerabilities. Evidence related to cybercrime, and in fact related to any crime, may be stored on all types of computers or storage device. Any law enforcement officer, prosecutor or judge will thus be confronted with electronic evidence sooner or later.¹⁶ Capacity building programmes can help criminal justice authorities to meet these challenges, for example, through training and institution building and by mainstreaming the issues of cybercrime and electronic evidence into law enforcement and judicial training curricula.
- Contribution to cybersecurity. Many governments are adopting cybersecurity strategies with the primary purpose of protecting critical information infrastructure. Capacity building programmes on cybercrime can support a crucial element of cybersecurity strategies, namely the criminal justice response to attacks against the confidentiality, integrity and availability of computers. Cybersecurity is increasingly considered a matter of national security. A stronger focus on the criminal justice response to cyber attacks may help take cybersecurity out of the “national defense corner” and help establish rule of law and human rights safeguards also with respect to cybersecurity.
- Protecting people against crime and protecting their rights. Capacity building programmes can help governments meet their positive obligation to protect people against crime. This includes protecting people against murder, trafficking in human beings, sexual violence (including against children) and other types of violent crime, against corruption, drug trafficking, extortion, stalking, theft or fraud that may all take place in the real world but involve electronic evidence. At the same time, when governments take action against cybercrime they must respect rule of law and human rights requirements. Investigative powers must be limited by conditions and

¹⁴ <http://www.internetworldstats.com/stats.htm>

¹⁵ For example, Uganda had some 14 million subscriptions to mobile phones in 2011 (<http://www.freedomhouse.org/report/freedom-net/2012/uganda>) and allegedly “there are mobile phones in Uganda than lightbulbs”. People use mobile phones to make payments also in remote rural areas. In Kenya alone, more than 17 million people are reported to use “M-Pesa” for payments.

¹⁶ This is not only true for criminal cases but commercial law, labor law, civil proceedings etc.

safeguards.¹⁷ The preservation, analysis and presentation of electronic evidence must follow clear rules to serve as evidence in court (chain of custody). Capacity building programmes should furthermore strengthen regulations and mechanisms for the protection of personal data. This is particularly important given that the most private data of individuals are nowadays stored in electronic form. In short, such programmes can not only help protect people against crime but also their rights.

- Contribution to human development and democratic governance. Capacity building programmes on cybercrime in turn may help societies exploit ICT as “powerful tools for human development and poverty reduction”¹⁸. Strengthening confidence, trust, security and reliability of ICT will facilitate economic development and access to education and sharing of information. Effective criminal justice systems will enhance the physical security and health of individuals, for example, by protecting children against sexual exploitation and abuse, by preventing the distribution of counterfeit and substandard medicines or by protecting people against crime in general. Criminal justice measures based on law and meeting rule of law requirements will contribute to democratic governance and reduce undue interference in the rights of individuals as well as the risk of abuse of power.

¹⁷ http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2467_SafeguardsRep_v18_29mar12.pdf

¹⁸ UNDP (2001): Human Development Report 2001 – Making new technologies work for human development. New York. <http://hdr.undp.org/en/media/completnew1.pdf>

4 Objectives of capacity building programmes

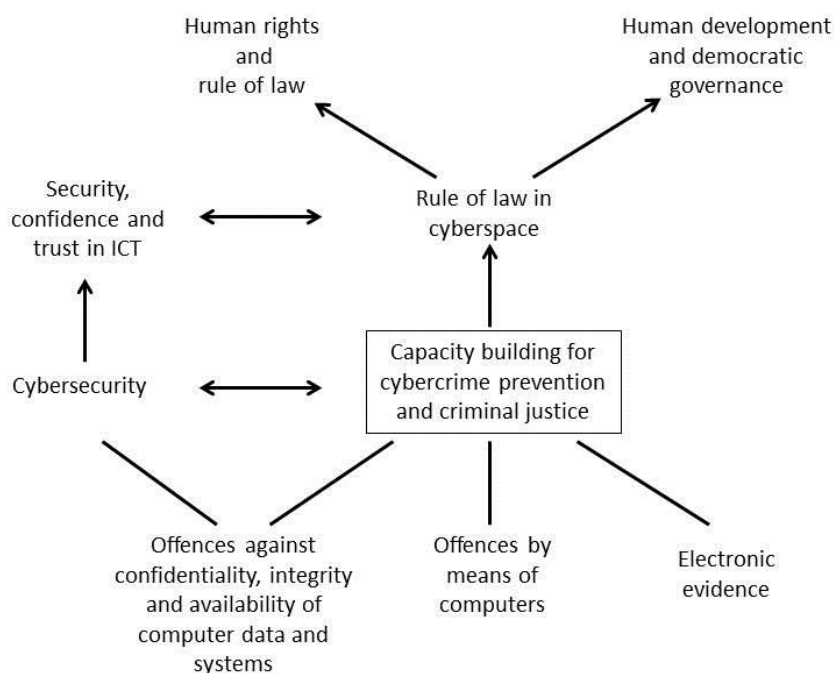
4.1 Rationale and objectives

Programmes on cybercrime should contribute to the overall objective of strengthening the rule of law in cyberspace. This in turn is to contribute to human rights, the rule of law, democratic governance and human development as well as the security, confidence and trust in ICT.

This implies that programmes should not only reinforce safeguards to prevent unintended consequences such as the abuse of law enforcement powers but should aim at human rights, the rule of law and human development as an intended outcome.

The direct objective of such programmes should be to strengthen a criminal justice response with regard to:

- offences against the confidentiality, integrity and availability of computer data and systems;
- offences by means of computers;
- electronic evidence stored on computers in relation to any crime.



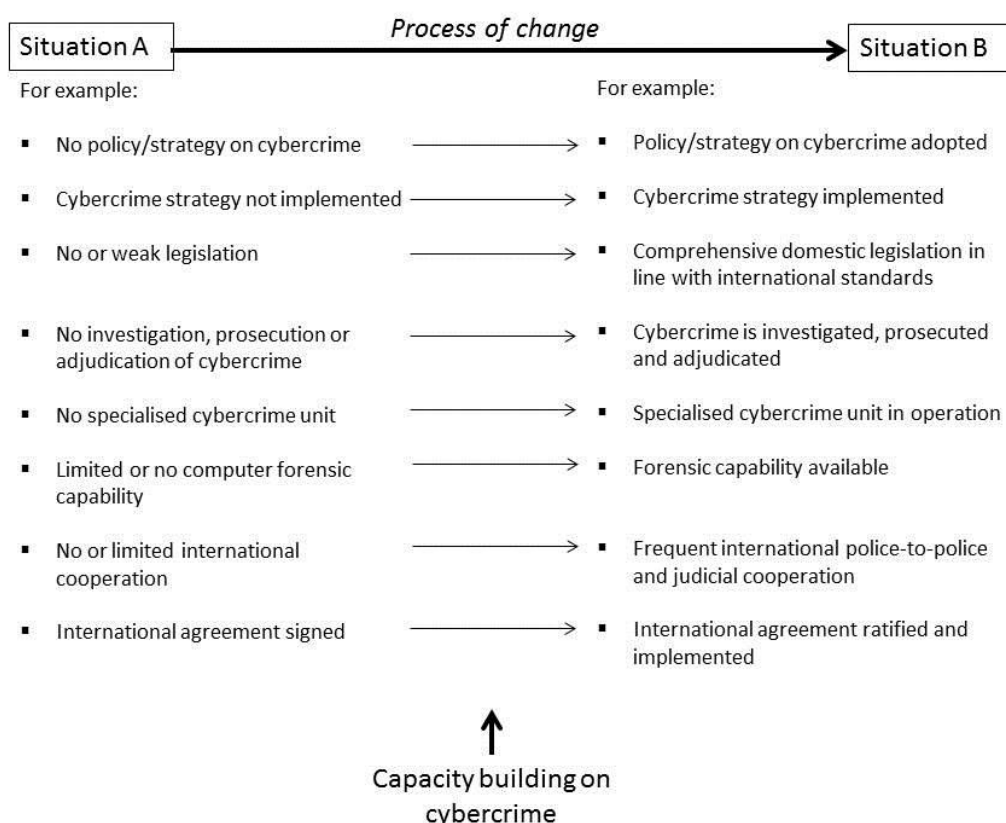
Cybercrime and electronic evidence are transversal and transnational challenges requiring cooperation at all levels: interagency, public/private (in particular law enforcement/Internet service provider) and international cooperation. The strengthening of cooperation should thus be reflected in the objectives of any capacity building programme in this sector.

4.2 Supporting a process of change

Programmes on cybercrime – like all technical cooperation or capacity building programmes – are to support processes of change.

Such processes, their objectives and expected outcomes are to be defined and owned by the organisation or government receiving support. Without such a commitment and a clearly defined process of change, capacity building risks resulting in parallel processes or structures that are not sustainable.

For example, a donor may organise an ad-hoc training course for judges and prosecutors. Such a training course may be of some benefit for participants, but in all likelihood be of limited impact and results will soon evaporate. It is not excluded that another donor will then organise a similar course. If on the other hand, a government or a judicial training institution is committed to enhancing the skills of judges and prosecutors with respect to cybercrime and electronic evidence, a capacity building programme may support a training institution in the development of training materials, the training of trainers and the delivery of pilot courses so that such training is integrated into the curricula of training institutions. If a government or training institution has a defined strategy, different donors may be able to provide support in a complementary manner.



From the perspective of the Council of Europe, the intention of a government to implement the Budapest Convention on Cybercrime represents a commitment to a process of change. An official request for accession to the Budapest Convention justifies resource mobilisation for capacity building activities aimed at supporting full implementation of this treaty.

5 Elements of capacity building programmes

Experience suggests that capacity building programmes for cybercrime prevention and criminal justice could address the following:

5.1 Cybercrime policies and strategies

Support to governments and organisations in views of the adoption and implementation of comprehensive and coherent policies and strategies on cybercrime, including:

- Engagement of decision-makers. It is essential that decision-makers in government and organisations understand risks and options, agree on strategic priorities, provide political backing and allocate resources to measures on cybercrime.
- Synergies and links with cybersecurity strategies. Strategies on cybercrime and cybersecurity strategies are interrelated and mutually reinforcing. Cybersecurity strategies often comprise measures on cybercrime. Synergies and links between both need to be established.
- Multi-stakeholder participation. Approaches on cybercrime require the cooperation of multiple stakeholders within the public sector but also the private sector.
- Human rights and rule of law requirements. A criminal justice response to cybercrime implies a rule of law rationale which means that human rights and rule of law requirements are not only to be met but to be promoted.
- Management of cybercrime strategies. Such strategies need to be operationalised, implementation needs to be well managed, coordinated and monitored, and the progress, results and impact need to be assessed to permit corrective measures and justify the allocation of resources.
- Contributions by donors and cooperation with partners. A clear policy or strategy on cybercrime allows donors and other partners to provide support as it defines the process of change to be undertaken (from a "Situation A" to a Situation "B") and the outcomes expected.

Many donors require a policy to be in place before approving technical assistance and capacity building programmes. On the other hand, a programme may also have as objective the development of a strategy on cybercrime.

As indicated above, from the perspective of the Council of Europe, an official request for accession to the Budapest Convention on Cybercrime represents a commitment of a government that justifies capacity building activities which are then to support full implementation of this treaty.

Resources/examples:

- [Cybercrime strategies](#)
- [Strategic priorities on cybercrime in South-eastern Europe](#)

5.2 Legislation

Criminal justice measures on cybercrime and electronic evidence must be based on law. Public authorities should, therefore, be supported in the strengthening of their domestic legislation:

- Substantive law measures to criminalise offences against computer data and systems (including as a minimum illegal access, illegal interception, data and system interference, misuse of devices) and by means of computers (including as a minimum computer-related forgery and fraud, child pornography and other forms of sexual violence against children, violations of intellectual property rights and related rights by means of computers if committed on a commercial scale).
- Procedural law tools permitting efficient investigations and use of electronic evidence in criminal proceedings. This should include as a minimum the admissibility of electronic evidence in criminal proceedings, the expedited preservation of data, production orders, search and seizure of stored computer data, real-time collection of traffic data and the interception of content data for specified investigations.
- Safeguards and conditions for the use of investigative powers. Procedural law powers need to be provided for specified investigations – as opposed to general surveillance – and must be limited by safeguards and conditions to prevent their abuse, such as the principle of necessity and proportionality, judicial or other independent supervision, grounds justifying application of the power and others. Moreover, governments should adopt a framework for the protection of personal data to provide for further safeguards.
- A sufficient level of harmonization of domestic legislation with international standards to facilitate international cooperation.

Resources/examples:

- [Budapest Convention on Cybercrime, including Explanatory Report](#)
- [Country profiles on cybercrime legislation](#)
- [Article 15 Conditions and safeguards under the Budapest Convention on Cybercrime](#)
- [Internet: case law of the European Court of Human Rights](#)
- [Data protection – Compilation of Council of Europe texts](#)

5.3 Cybercrime reporting

Limited data and knowledge on cybercrime is a key obstacle to the prevention and control of cybercrime, and makes it difficult to obtain political commitment and resources. Public authorities should thus be supported in:

- Establishing reporting channels for individuals and public and private sector organisations. Reports may trigger law enforcement investigations, provide intelligence for a better understanding of scope, threats and trends of cybercrime, and allow for collating data to detect patterns of organised criminality.

Resources/examples:

- [Internet Crime Complaint Center](#)
- [National Fraud Reporting Centre](#)
- [Signal Spam](#)

5.4 Prevention

In addition to technical, administrative and procedural measures to protect computer systems, public education and awareness are essential elements to prevent cybercrime. Support may be provided to:

- Public websites with information on cybercrime prevention, educational materials and courses, recommendations for employees of public or private sector organisations, resources to prevent risks in a specific sector or organisation or assistance to victims of cybercrime;
- Combining cybercrime reporting channels with information on preventive measures and threat alerts. Internet service providers may run platforms with targeted information for users whose systems are infected as well as assistance in the cleaning up of user systems.

Resources/examples:

- www.botfrei.de
- www.ic3.gov/preventiontips.aspx
- <http://www.actionfraud.org.uk/home>

5.5 Specialised units

The investigation of cybercrime and forensic analysis of electronic evidence and the prosecution of cybercrime require specific skills. Criminal justice authorities should thus be supported in the setting up or strengthening of:

- Police-type cybercrime or high-tech units with strategic and operational responsibilities;
- Prosecution-type cybercrime units;
- Computer forensic capabilities within cybercrime units or as separate structures;
- Skills within the judiciary. The creation of specialized courts may be considered where this is compatible with the legal system of the country;
- Interagency cooperation. This is essential as cybercrime units are to cooperate with other police services (such as economic crime units, child protection units) and institutions (such as financial intelligence units, Computer Emergency Response Teams and others).

Resources/examples:

- [Specialised cybercrime units – Good practice study](#)

5.6 Law enforcement training

Crimes increasingly involve computer systems or electronic evidence on computers or storage devices. Any law enforcement officer, prosecutor or judge will sooner or later need to deal with electronic evidence. Support should therefore be provided to comprehensive law enforcement training, including:

- Sustainable, standardised, replicable, scalable training;
- Skills to investigate cybercrime, secure electronic evidence, carry out computer forensic analyses, assist other agencies and contribute to network security;
- Skills/competencies required for respective functions and at appropriate level (from first responder to forensic investigators);
- Cooperation for training purposes between law enforcement, academia and industry;
- Use of existing law enforcement training materials and initiatives.

Resources/examples:

- [Law enforcement training strategies](#)
- [Electronic evidence guide](#)
- www.2centre.eu/
- [European Cybercrime Training and Education Group \(ECTEG\)](#)

5.7 Judicial training

Not only law enforcement officers but also most if not all prosecutors and judges need to be able to deal with cybercrime and electronic evidence. While at the level of the police, specialised cybercrime units are often established that offer technical support to other police services, the creation of specialised prosecution services is less widespread and very rare within the judiciary (principle of the “natural judge”). The lack of knowledge and skills among prosecutors and in particular judges seems to be a major concern in most countries and in all regions of the world. Regular judicial training on cybercrime and electronic evidence is very rare. Programmes should support training to allow prosecutors and judges to acquire the necessary skills regarding cybercrime and electronic evidence:

- Initial and in-service training for judges and prosecutors by training institutions on cybercrime and electronic evidence. This includes the preparation of training materials or the adaptation of existing materials to the needs of a jurisdiction, the training of trainers in the delivery of training, the mainstreaming or insertion of such training modules into the regular curricula of judicial training institutions to ensure sustainability;
- Advanced training for a critical number of judges and prosecutors;
- Further specialisation and technical training of judges and prosecutors;
- Enhanced knowledge through networking among judges and prosecutors and making available of case law and other resources.

It may furthermore be important to train lawyers, solicitors and advocates, in particular in common law countries where they are officers of the court. This will contribute to the rule of law and strengthen safeguards.

Resources/examples:

- [Cybercrime training for judges and prosecutors: a concept](#)
- [Introductory course for judges and prosecutors](#)
- Advanced course for judges and prosecutors
- [Electronic evidence guide](#)

5.8 Public/private cooperation

Public/private cooperation and information exchange has a strong impact on the prevention and control of cybercrime and the securing of electronic evidence for criminal proceedings. This includes in particular cooperation between law enforcement authorities and Internet service providers (ISP) but also with financial sector institutions and other industry sectors as well as with Computer Emergency Response Teams/Computer Security Incident Response Teams (CERT/CSIRT), academia, non-governmental initiatives (such as for child protection) and others. Programmes should support:

- Strengthening of law enforcement/ISP cooperation;
- Creating information and intelligence sharing centres (ISAC) for the financial and other sectors;
- Setting up of cybercrime reporting systems (such as for spam, botnets, child abuse materials);
- Law enforcement /CERT or CSIRT cooperation;
- Private/public information sharing in line with data protection requirements.

Resources/examples:

- [Law enforcement/ISP cooperation guidelines](#)
- [National Cyber-Forensic and Training Alliance \(NCFTA\)](#)
- [Financial Sector ISAC](#)

5.9 International cooperation

Cybercrime is transnational in nature; volatile electronic evidence needs to be secured in multiple jurisdictions. Programmes should, therefore, enable competent authorities (Ministries of Justice, prosecution services, law enforcement) to engage in efficient international cooperation:

- Strengthening domestic legislation as a basis for international judicial and police-to-police cooperation;
- Setting up 24/7 points of contact for urgent international cooperation, in particular data preservation;

- Training and networking of authorities for mutual legal assistance;
- Ratification of or accession to international treaties and conclusion of bi-lateral agreements.

Resources/examples:

- [Budapest Convention on Cybercrime \(Chapter III\)](#)
- [24/7 points of contact](#)

5.10 Protection of children

Sexual violence and other threats against children online are major concerns worldwide. Increasingly such violence involves information technologies. Programmes should support measures against the sexual exploitation and abuse of children online:

- Comprehensive approaches ranging from prevention to protection and prosecution;
- Public/private cooperation;
- Strengthening of legislation in line with international standards;
- Creating conditions for effective enforcement to prosecute offenders and rescue victims.

Resources/examples:

- [Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse](#)
- [Promoting children's rights and protecting children from violence](#)
- [Criminal law benchmarks of the Lanzarote and Budapest Conventions](#)

5.11 Financial investigations and prevention of fraud and money laundering

Most cybercrime is aimed at obtaining illicit financial benefits. Targeting crime proceeds and searching, seizing and confiscating criminal money on the Internet and the prevention of money laundering can be a powerful strategy. Programmes should, therefore, support:

- Cooperation between cybercrime, financial investigation and financial intelligence units as well as the financial sector;
- Financial investigations in parallel to cybercrime investigations;
- Implementation of international standards on money laundering and the search, seizure and confiscation of proceeds from crime;
- Risk management and due diligence in the financial sector.

Resources/examples:

- [Criminal money flows on the Internet](#)
- [MONEYVAL](#)
- [Financial Action Task Force](#)

5.12 Prevention and control of terrorist use of ICT

Terrorists may use information technologies for attacks on critical infrastructure, the dissemination of illegal contents, including threats, incitement to terrorism or recruitment and training, for logistical purposes or for the financing of terrorist activities. Programmes should support:

- The strengthening of legislation on cybercrime, including procedural law and on electronic evidence, and terrorism in line with international standards;
- Training and other institution building measures;
- Interagency cooperation;
- Implementation of measures on terrorist financing;
- Implementation of guidelines on human rights and the fight against terrorism.

Resources/examples:

- [Budapest Convention on Cybercrime](#)
- [Cyberterrorism website](#)
- [Convention on the Prevention of Terrorism](#)
- [Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and the Financing of Terrorism](#)
- [Guidelines on human rights and the fight against terrorism](#)

6 Sequencing

Capacity building programmes should be implemented in a pragmatic manner and there may thus be many ways to sequence activities.

A programme should support a government or an organisation in a country in a process of change. Obviously, this government or the organisation should therefore make a request for assistance and should determine the way the assistance is to be provided. Assistance should not be donor driven.

The strengthening of legislation on cybercrime and electronic evidence is a suitable starting point to enter into dialogue with a government. The intention of a government to prepare a law or to reinforce existing legislation reflects a commitment to reform that can be supported through a capacity building programme with the adoption of a law as objective or expected result. Supporting law reform first is sensible since criminal justice is to be based on law. On the other hand, starting cooperation, for example, with computer forensic training courses or with the training of judges without a legal framework on cybercrime and electronic evidence in place may be of limited use.

Experience shows that engagement of decision-makers is essential for the success of capacity building programmes and for criminal justice measures on cybercrime in general. A thorough analysis of the cybercrime situation and of the strengths and weakness of criminal justice capabilities will facilitate the engagement of decision makers and will establish benchmarks against which progress can be determined later on.

Towards the end of a programme (or of a phase of a programme) progress made should be assessed. The outcome of such an assessment should then be fed back into policies and strategies and reconfirm the engagement of decision-makers beyond the completion of the programme. For example, decision-makers could commit to future strategic priorities on cybercrime.¹⁹ This should contribute to the sustainability of the process of change supported by the programme.

Example: Sequencing of the CyberCrime@IPA project²⁰



¹⁹ See for example:

http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy%20project%20balkan/Strategic_priorities_conference/2467_Strategic_Priorities_V16_final_adopted.pdf

²⁰ Joint project of the European Union and the Council of Europe on Cybercrime in South-eastern Europe (see below for details). The CyberCrime@IPA and GLACY follow a similar logic.

7 Capacity building: the experience of the Council of Europe

7.1 Overview²¹

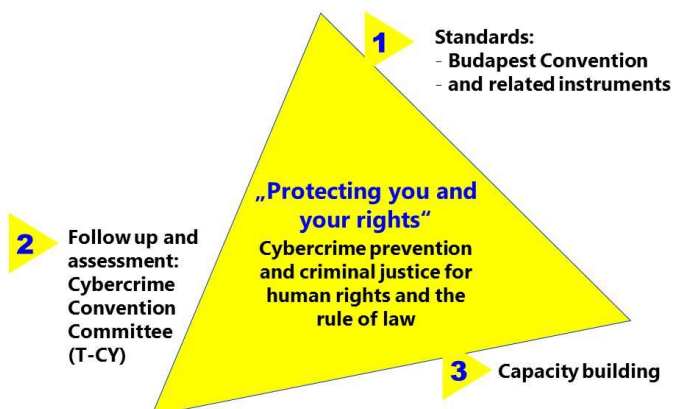
The approach of the Council of Europe on cybercrime consists of the three interrelated elements of the setting of common standards, follow up and assessment of implementation, and technical cooperation for capacity building.²²

Standards include in particular the [Budapest Convention on Cybercrime](#) but also its [Additional Protocol on Xenophobia and Racism committed by means computer systems](#), as well as treaties on data protection ([Convention 108](#)), on the sexual exploitation and sexual abuse of children ([Lanzarote Convention](#)), on [money laundering and the financing of terrorism](#) and others.

The Cybercrime Convention Committee ([T-CY](#)) represents the Parties to the Budapest Convention ("Consultations of the Parties"), interprets the text of the Convention, prepares Guidance Notes and, importantly, assesses its implementation.

In this dynamic triangle, capacity building is aimed at assisting governments and organisations in the implementation of the Budapest Convention and related standards, including human rights and rule of law principles, and in following up on the assessments carried out by the T-CY. Results of capacity building in turn inform standard setting and the work of the T-CY.

A range of country-specific, regional and global capacity building projects has been carried out by the Council of Europe since 2006. Additional projects are in preparation. Many projects are co-funded by the European Union. The EU supports the Budapest Convention and capacity building on cybercrime worldwide.

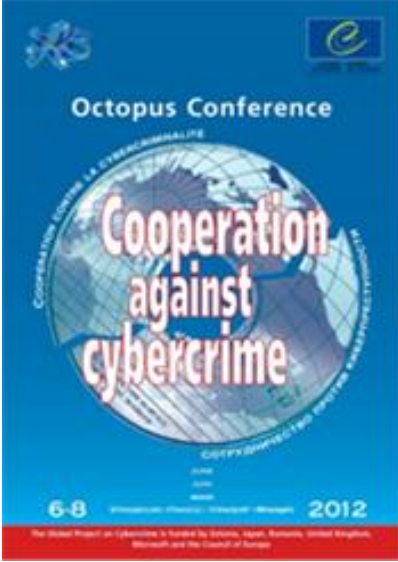


²¹ For an overview of activities in 2012 see:

http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/cyber_coe_actrep2012_v1provisional.pdf

²² The approach on cybercrime in turn is part of an Internet Governance Strategy of the Council of Europe <https://wcd.coe.int/ViewDoc.jsp?Ref=CM%282011%29175&Language=lanEnglish&Ver=final&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383>

7.2 Projects

Title:	Global Project on Cybercrime (Phase 1)
Project area:	Worldwide (more than 100 countries involved)
Duration:	2006 – 2009
Budget:	EUR 1.1 million
Funding:	Estonia, Microsoft and the Council of Europe
Implementation:	Council of Europe
Objective:	To promote broad implementation of the Convention on Cybercrime (CETS 185) and its Protocol on Xenophobia and Racism (CETS 189), and to deliver specific results in terms of legislation, criminal justice capacities and international cooperation.
Summary of results:	<p>Some 110 activities were organised or supported in all regions of the world. The project in particular assisted in legislative reforms and helped establish the Budapest Convention as the primary standard of reference for cybercrime legislation globally. Results also included the preparation of Guidelines for law enforcement / Internet service provider cooperation and the strengthening of 24/7 points of contact for urgent international cooperation. Multi-stakeholder cooperation was supported through the annual Octopus Conferences organised under this project. The final project report is available at:</p> <p>http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20Project/567-d-final%20report1i%20final%20_15%20june%2009_.pdf</p>
	
	<p>Octopus Conferences on cooperation against cybercrime have been organised since 2004 and bring together public and private sector stakeholders from all over the world.</p> <p>Since 2007, Octopus Conferences have been part of the Global Project on Cybercrime.</p> <p>In 2012, an online "Octopus Community" was set up as an additional platform for experience exchange.</p>

Title:	Global Project on Cybercrime (Phase 2)
Project area:	Worldwide (more than 100 countries)
Duration:	2009 – 2011
Budget:	EUR 1 million
Funding:	Estonia, Japan, Monaco, Romania, Microsoft, McAfee, Visa Europe and the Council of Europe
Implementation:	Council of Europe
Objective:	To promote global implementation of the Convention on Cybercrime (CETS 185) and its Protocol on Xenophobia and Racism (CETS 189) and related international standards on data protection (CETS 108, CETS 181) and the online sexual abuse of children (CETS 201)
Summary of results:	<p>Some 130 activities were organised in support of seven expected results (1. Legislation and policies, 2. International cooperation and 24/7 contact points, 3. Law enforcement/ISP cooperation, 4. Financial investigations, 5. Judicial training, 6. Data protection and privacy, 7. Protection of children against online sexual violence). The project served as the primary tool to support implementation of the Budapest Convention worldwide. It facilitated accession requests and an increase in the number of Parties to this treaty. The project promoted multi-stakeholder cooperation, among other things, through annual Octopus conferences. Some 120 countries and more than 100 private sector, civil society organisations academia participated in project activities. The project fed into the work of the Cybercrime Convention Committee (T-CY) and contributed to global discussions on capacity building on cybercrime.</p> <p>The final project report is available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_adm_finalreport_V12_9apr12.pdf</p>

Title:	Joint Project on Cybercrime in Georgia
Project area:	Georgia
Duration:	2009 – 2010
Budget:	EUR 220,000
Funding:	Joint project of the European Union and the Council of Europe
Implementation:	Council of Europe
Objective:	To contribute to the security of and confidence in information and communication technologies in Georgia and to help Georgia develop a consistent policy on cybercrime in view of implementing the Convention on Cybercrime (CETS 185)
Summary of results:	<p>Legislative amendments on cybercrime and data protection prepared with the support of this project were subsequently adopted by Parliament, and Georgia became a Party to the Budapest Convention on Cybercrime. A judicial training concept was adopted and a train-the-trainers course was carried out. A concept for a high-tech crime unit was prepared and a decision in this respect was taken by the Government. The unit was then established following the completion of the project. A memorandum of understanding was concluded on the cooperation between law enforcement and Internet service providers.</p> <p>The final project report is available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_project_in_georgia/2215_d_Final_Narrative_Report_Georgia.pdf</p>

Title:	CyberCrime@IPA Joint Project on Cybercrime in South-eastern Europe
Project area:	Albania, Bosnia and Herzegovina, Croatia, Montenegro, Serbia, "The former Yugoslav Republic of Macedonia", Turkey and Kosovo* ²³
Duration:	2010 – 2013
Budget:	EUR 2.77 million
Funding:	European Union (Instrument of Pre-Accession, IPA) and Council of Europe
Implementation:	Council of Europe
Objective:	To strengthen the capacities of criminal justice authorities of Western Balkans and Turkey to cooperate effectively against cybercrime
Summary of results:	<p>CyberCrime@IPA produced results in eight fields: 1. Cybercrime policies and strategies, 2. Harmonisation of legislation, 3. International cooperation, 4. Law enforcement training, 5. Judicial training, 6. Financial investigations, 7. Law enforcement/ISP cooperation, 8. Assessments (see case study).</p> <p>This project comprised most of the elements listed above. The concepts and materials developed (Electronic Evidence Guide, 1st Responder training, basic and advanced judicial training courses) are adaptable and replicable in any region.</p> <p>In terms of methodology, a situation report was prepared at the outset and decision-makers participated in the launching conference. Towards the end of the project a peer-to-peer assessment was carried out to determine progress made. The results fed into a set of strategic priorities adopted by ministers and senior officials of countries and areas participating in the project.</p> <p>The assessment report on progress made in this region is available at: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy%20project%20balkan/2467_Assess_Rep%20v51_public.pdf</p>

Title:	CyberCrime@EAP Joint Project on Cybercrime in Eastern Partnership countries
Project area:	Armenia, Azerbaijan, Belarus, Georgia, Moldova, Ukraine
Duration:	2010 – 2013
Budget:	EUR 724,000
Funding:	European Union
Objective:	To strengthen the capacities of criminal justice authorities of Eastern Partnership countries to cooperate effectively against cybercrime in line with European and international instruments and practices
Summary of results:	<p>Eastern Partnership countries have defined strategic priorities regarding cybercrime and assessed measures taken. Eastern Partnership countries have been provided with the tools for action against cybercrime (legislation including rule of law safeguards, specialise cybercrime units, law enforcement and judicial training, law enforcement/ISP cooperation, financial investigations, international judicial and police-to-police cooperation including 24/7 points of contact). Eastern Partnership countries participate more actively in international cybercrime efforts.</p> <p>A progress report is available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_Project_EaP/2523_ProgressRep_25_April%2012fin.pdf</p>

²³ *This designation is without prejudice to positions on status, and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo* Declaration of Independence

Title:	Global Project on Cybercrime (Phase 3)
Project area:	Worldwide (more than 100 countries)
Duration:	2012 – 2013
Budget:	EUR 1 million
Funding:	Estonia, Japan, Monaco, Romania, United Kingdom, Microsoft and the Council of Europe
Objective:	To promote broad implementation of the Budapest Convention on Cybercrime (CETS 185) and related standards and tools
Summary of results:	<p>Legislative reforms were supported in countries of Africa, Americas and Asia-Pacific. A global review on the state of cybercrime legislation was carried out, and results fed into international discussions on cybercrime and capacity building. Awareness of safeguards and conditions regarding investigative powers was promoted. Studies on cybercrime strategies, on criminal money flows and on criminal law benchmarks for the protection of children against online violence were prepared and disseminated. Multi-stakeholder cooperation was promoted, among other things through Octopus conferences and participation in the Internet Governance Fora and European Dialogue on Internet Governance. The project supported the work of the Cybercrime Convention Committee (T-CY). Additional States became Parties to the Budapest Convention or requested accession.</p> <p>The project summary is available at: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_project_Phase3_2571/2571_Phase3_summary_V8_nov2012.pdf</p>

Title:	GLACY – joint project on Global Action on Cybercrime
Project area:	Worldwide (States prepared to implement the Budapest Convention)
Duration:	2013 – 2016
Budget:	EUR 3.35 million
Funding:	European Union (Instrument for Stability) and Council of Europe
Objective:	To enable criminal justice authorities to engage in international cooperation on cybercrime and electronic evidence on the basis of the Budapest Convention
Summary of expected results:	<ol style="list-style-type: none"> 1. Engagement of decision-makers: Decision-makers of project countries are aware of cybercrime threats and rule of law/human rights implications and have identified strategic priorities regarding cybercrime 2. Harmonisation of legislation: Amendments are drafted to bring domestic legislation fully in line with the Convention on Cybercrime (CETS 185) and to improve legislation and regulations on data protection and child online protection 3. Judicial training: Enhanced skills for judges and prosecutors regarding cases on cybercrime and electronic evidence 4. Law enforcement capacities: Enhanced specialised skills and institutions for investigations on cybercrime and electronic evidence 5. International cooperation: Enhanced international law enforcement and judicial cooperation against cybercrime based on Chapter III of the Budapest Convention on Cybercrime 6. Information sharing: Increased public/private and interagency information sharing in line with data protection standards 7. Assessment of progress: Governments are able to assess progress made in the investigation, prosecution, adjudication of cybercrime and cases involving electronic evidence, including international cooperation

Title:	CYBERCRIME@OCTOPUS
Project area:	Worldwide
Duration:	2014 – 2016
Budget:	EUR 1.8 million
Funding:	Voluntary contributions
Objective:	To support implementation of the Budapest Convention on Cybercrime (CETS 185)
Summary of expected results:	<ol style="list-style-type: none"> 1. Octopus conferences on cooperation against cybercrime Under this project future Octopus Conferences are to be organised. 2. Support to the Cybercrime Convention Committee (T-CY) This project will support the T-CY, including in particular the participation of observer States in the work of the T-CY. 3. Countries assisted in the implementation of the Budapest Convention The project will assist any country prepared to implement the Budapest Convention, in particular with regard to legislation and international cooperation.

7.3 C-PROC: Cybercrime Programme Office of the Council of Europe

With increasing demand for capacity building on cybercrime and electronic evidence, organisations providing support need to enhance their own capacities to engage in technical cooperation.

Further to an offer by the Prime Minister of Romania the Council of Europe, therefore, decided in October 2013 to establish a [Cybercrime Programme Office in Bucharest, Romania](#). The C-PROC will be responsible for the implementation of the capacity building projects of the Council of Europe on cybercrime and electronic evidence worldwide.

The added value includes specialisation, cost-effective project management, competitiveness and thus increased resource mobilisation.

The activities managed by C-PROC will remain closely linked to the work of the Cybercrime Convention Committee (T-CY) and other intergovernmental activities of the Council of Europe in Strasbourg, France.

8 Conclusions

Policy discussions at international levels show that capacity building on cybercrime can build upon broad political support.

Experience, good practices and success stories are available and are adaptable and replicable. They represent evidence that:

- Capacity building as an approach on cybercrime has a number of advantages. It responds to needs and produces immediate impact, favours multi-stakeholder cooperation, contributes to human development, poverty reduction and the rule of law, and helps reduce the digital divide.
- Elements of capacity building programmes may include support to cybercrime policies and strategies, legislation including rule of law safeguards, reporting systems and prevention, specialized units, law enforcement and judicial training, interagency cooperation, public/private cooperation, international cooperation, protection of children, and financial investigations.
- An effective criminal justice response is an essential component of a governance framework that is to ensure the security, confidence and trust in ICT so that societies are able to exploit the benefits of information and communication technologies for development.
- Capacity building programmes should, therefore, be designed to make a positive contribution to the rule of law and human rights in cyberspace and to contribute to cybersecurity (“protecting you and your rights”). In this logic, strengthening safeguards for law enforcement powers and frameworks for the protection of personal data are essential.
- Tangible impact comprises increased use of electronic evidence in criminal proceedings, increased numbers of investigations, prosecutions and adjudications, shorter response times to requests for mutual assistance, more efficient police-to-police cooperation and other verifiable indicators.
- The success of such programmes is also to be measured in terms of their contribution to human development and democratic governance.

However, while there is no doubt that ICT offer opportunities for human development (“enlarging people’s choices”), the link between capacity building on cybercrime and human development is not widely understood. The risk of cybercrime for countries in the South is still underestimated.

As a consequence, the issue of cybercrime is not yet on the development cooperation agenda, and development cooperation organisations are largely absent from this field. This may explain why the broad international support to capacity building on cybercrime at political levels has not yet been translated – with exceptions – into the mobilisation of adequate financial resources for such programmes. Bringing development cooperation organisations on board is thus a critical challenge ahead.

