Cybercrime@EAP
EU/Council of Europe Eastern Partnership Facility

Bucharest, 12 May 2015
Provisional

Cybercrime and cybersecurity strategies in the Eastern Partnership region

Results of a regional workshop
Chisinau, Republic of Moldova,
12 – 14 November 2014

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

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

Abbreviations

CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CIIP	Critical Information Infrastructure Protection
EAP	Eastern Partnership
EC3	Europol European Cybercrime Centre
ENISA	European Network and Information Security Agency
EU NIS	European Union Network & Information Security directive
FIRST	Forum of Incident Response and Security Teams
ICT	Information and Communication Systems and Technologies
IMPACT	International Multilateral Partnership Against Cyber Threats
iOCTA	Internet Organised Crime Threat Assessment
ISP	Internet Services Provider
ITU	International Telecommunication Union
KPI	Key performance indicator
LEA	Law Enforcement Agency
MLA	Multilateral Assistance
NATO	North Atlantic Treaty Organisation
NGO	Non-governmental organisation
OECD	Organisation for Economic Co-operation and Development
OSCE	Organisation of Security and Cooperation in Europe
SOCA	Serious Organized Crime Agency
UN	United Nations

Note:
This document has been prepared under the Cybercrime@EAP project by Monika Josi, Safis Consulting AG, Switzerland with additional contributions from Daniel Ionita, Romania, Markko Kunnapu, Estonia, Virgil Spiridon, Romania and Giorgi Tielidze, Georgia.

1 Introduction

1.1 About CyberCrime@EAP

The purpose of this report is to promote the adoption and implementation of cybercrime and cybersecurity strategies in the Eastern Partnership region. The report is one outcome of a regional conference held in Chisinau, Republic of Moldova, from 12 to 14 November 2014.[1]

Through the Cybercrime@EAP project, between 1 March 2011 and 31 December 2014, the Council of Europe and the European Union supported States participating in the Eastern Partnership Facility (Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine) to strengthen their capacities to cooperate effectively against cybercrime in the areas of:

- Policies and awareness of decision-makers;
- Harmonised and effective legislation;
- Judicial and law enforcement training;
- Law enforcement – Internet service provider cooperation;
- International judicial and police cooperation;
- Financial investigations.

At a meeting in Kyiv, Ukraine, 31 October 2013, participating States adopted the following strategic priorities:

- 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.

Furthermore, the Cybercrime@EAP assessment report[2] (2013) suggested that although good progress had been made in the countries participating in the project, further action was required including with regard to the adoption of 'cybercrime policies and strategies;' (§7.9 of the Assessment Report).

---

1 http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_Project_EaP/Chisinau_International_Conference_Nov2014/EAP_Chisinau_WS.asp

2 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_Project_EaP/2523_strategic-priority-conf-Programme_v2.pdf

At an international conference in Chisinau, Moldova, organised by the Council of Europe, from 12 to 14 November 2014[3], States participating in the Eastern Partnership presented the status of the development or implementation of their strategies.

1.2 Objectives and terminology

1.2.1 Objectives

This report describes and analyses national and regional approaches to cybercrime and cybersecurity strategies as a form of policy making to effectively cooperate against cybercrime in the EAP region. It highlights the distinctions as well synergies between approaches to cybercrime and cybersecurity and makes overall conclusions and recommendations for further action. The report is based on information made available by the EAP countries and does not assess the actual implementation status for each country.

This study is intended to be of value to the EAP countries looking to develop and enhance cybercrime and cybersecurity strategies and brings to bear experience of neighbouring EU states (Czech Republic, Estonia and Romania).

1.2.2 Terminology: cybercrime versus cybersecurity

The terms cybercrime and cybersecurity are often used interchangeably. For the purpose of this report, definitions of cybercrime and cybersecurity, as stated in the discussion paper 'Cybercrime strategies' (30 March 2012[4]), will be used:

- Cybersecurity addresses
  - non-intentional incidents caused by malfunctioning of technology, coincidental failures, human failures, natural disasters and others;
  - intentional attacks by State and non-State actors, including botnet attacks to disrupt information infrastructure, unauthorised access and interception of data and communications (including computer espionage) or the manipulation or destruction of data and systems (including computer sabotage).

- Cybercrime (titles 1 and 2 of Budapest Convention) covers
  - offences against the confidentiality, integrity and availability of computer data and systems, that is, offences against computer data and systems, including illegal access, illegal interception, data and system interference, misuse of devices;
  - offences committed by means of computer systems. This list is limited to those 'old' forms of crime that obtain a new quality through the use of computers, that is, computer-related forgery and fraud, child pornography and offences related to infringements of copyright and related rights on a commercial scale.

The questions of cybersecurity and cybercrime are thus closey connected with regard to intentional attacks against computer data and systems. Cybersecurity and cybercrime are mutually reinforcing even though they follow a different rationale:

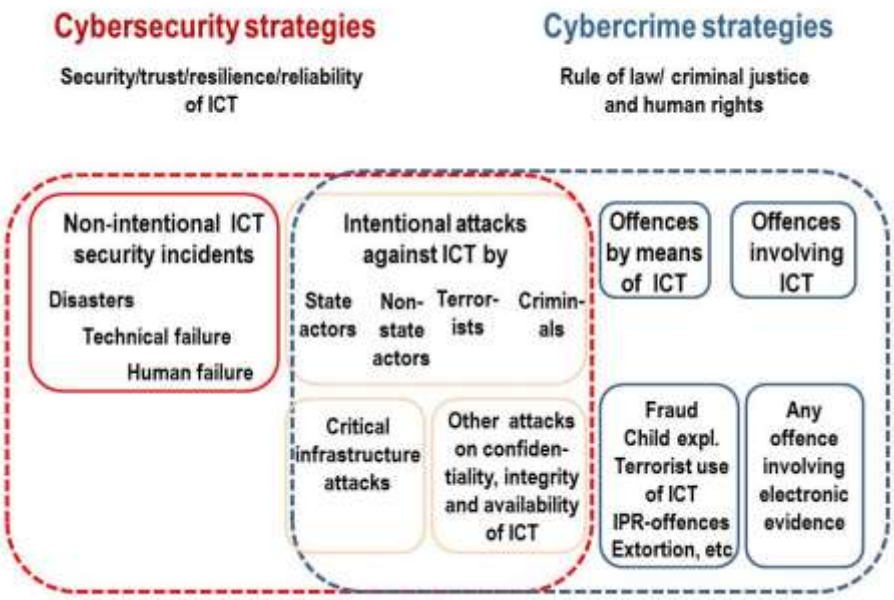
- A cybersecurity strategy is primarily aimed at the protection of the confidentiality, integrity and availability of computer data and systems in order to enhance security, resilience, reliability and trust in ICT.

[3] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_Project_EaP/Chisinau_International_Conference_Nov2014/EAP_Chisinau_WS.asp

[4] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_cy_strats_rep_V20_14oct11.pdf (especially pp. 6-7)

- A cybercrime strategy follows a criminal justice and rule of law rationale and is primarily aimed at the protection against

  - Intentional attacks against and by means of computers;
  - Any crime involving electronic evidence on a computer system.



1.3 Current threat landscape

The Internet has become a global infrastructure for both business and governments. In its 9th Global Risk Report[5], the World Economic Forum listed large-scale cyber-attacks, the breakdown of critical infrastructure and networks as well as massive incident of data fraud/theft amongst the top risks. Thus, cybersecurity has become a priority for many governments around the world. Cybersecurity also plays a very important role in cybercrime prevention. Cybersecurity measures i.e. security measures to protect the confidentiality, integrity and availability of computer data, to prevent crime can be interpreted differently by private and public stakeholders. For businesses, cybersecurity is about ensuring the availability of critical business functions and the protection of confidential data. For governments, it is mostly about protecting critical infrastructure and government computer systems from attacks, the breach of sensitive data affecting public safety and national security, while respecting the rule of law, data privacy, freedom of expression and human rights.

Furthermore, the threat environment has shifted for public and private sector entities tasked with the protection of critical infrastructure and sensitive information insofar as it can no longer be assumed that a system can be adequately protected against advanced targeted attacks. There is no such thing as absolute security, but individuals, businesses and governments must do everything to make criminal attacks as difficult as possible and to prepare for them. It is therefore paramount that all stakeholders not only invest in the direct protection of ICT (Information and Communication Systems and Technologies) but also invest in detection and response capabilities regarding threats. It is equally important to have in place the necessary legal and organisational frameworks enabling and facilitating cooperation and information exchange between national authorities and the private sector.

[5] http://www.weforum.org/reports/global-risks-2014-report

All countries in the EAP region face similar threats in cyberspace as other counties, which can be grouped into four main categories:

- Conventional cybercrimes: these crimes include both offences against the confidentiality, integrity and availability of computer data and systems as well as offences committed by means of ICT. These include fraud, theft of intellectual property or financial instruments, abuse or damage of protected information technology systems, and even damage of critical infrastructure. These crimes span those committed by individual hackers through those committed by organized crime entities, notably the rise of Crime as a Service, thus lowering entry barriers to cyberspace for criminals.[6]
- Military and political espionage/cyber attacks: these attacks include instances in which State entities intrude into, attempt to obtain or succeed in obtaining large amounts of sensitive data from government agencies or the military-industrial base or disrupt national critical infrastructure. This can also be done using a third-party to perform the attack.
- Economic espionage: this applies to States organising the theft of information and intellectual property owned by third parties or tolerating/enabling such theft by domestic companies from foreign competitors.
- Cyber conflict or cyber warfare: with all its benefiting factors, the internet also makes it possible for anonymous and difficult-to-trace individuals or organisations with resources to engage a nation-State in cyber conflict.

An additional emerging threat is posed by 'hactivism.' Increasingly, individuals and groups commit cybercrimes to gain publicity and notoriety, as an expression of protest, or to discredit a business or institution.

What is specific to the EAP region is its use as a platform to carry out cybercrime activities with targets elsewhere. According to the 2014 Internet Organised Crime Threat Assessment ('iOCTA'[7]) prepared by Europol's European Cybercrime Centre (EC3), the ICT infrastructure of several Eastern Partnership countries serves to host malicious content such as exploit kits, as well as other malware and phishing sites. Certain countries of the region are known to host botnet command and control servers, and to serve as bases for many highly technical cybercriminals (e.g. malware developers) who provide illicit services in the 'digital underground'.[8] The volume of malicious 'app' downloads is reportedly very high, compared to other parts of Europe.

Critical Infrastructure is often owned by the private sector: financial services (banking, insurance, credit card companies), utilities sector (electric, gas, oil and water firms), transport sector (fuel supply, railway network, airports, and harbours, inland shipping), telecommunications sector (ISP, communication including mobile communication providers), food sector (agriculture, food production and distribution), medical sector (this is a non-exhaustive list since the specification depends on the country). It may also involve economical sectors and industry.Therefore, its involvement in both cybercrime preventive measures and cybersecurity aspects has increased. In addition to sector specific security standards, i.e. finance and banking, governments can establish additional standards to enhance protection.

[6] https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta

[7] https://www.europol.europa.eu/sites/default/files/publications/iocta-epub.epub

[8] See iOCTA report (2014), especially pp. 66-67.

1.4 Outline of the report

Section 2 describes the methodology for evaluating current comparative developments regarding cybersecurity and cybercrime strategies outside the EAP region:

- For cybersecurity strategies, information from across the European Union (EU NIS Directive, ENISA, Czech Republic, Estonia, Netherlands, UK) is considered;
- For cybercrime strategies, the UK strategy is considered.

In light of these developments, the report describes the assessment criteria in section 2.3. These elements will be used to assess the status within the EAP countries.

In sections 3 – 8, individual EAP member countries will be briefly assessed.

Section 10 presents recommendations for implementation by the EAP countries in cyberspace.

2 Assessment methodology based on current developments

Considering the high risk of cyber threats, a number of European countries outside the EAP region have intensified their counter-efforts and are drafting or implementing strategies on cybersecurity.

2.1 Developments in the cybersecurity policy area

2.1.1 European Union Cybersecurity Strategy

The EU Cybersecurity Strategy[9] outlines the European Union's vision to promote an open, safe and secure cyberspace. The approach is articulated through five strategic priorities:

- Achieve cyber resilience;
- Drastically reduce cybercrime;
- Develop cyberdefence policy and capabilities;
- Develop the industrial and technological resources for cybersecurity;
- Establish a coherent international cyberspace policy for the European Union and promote core EU values.

To implement the strategy, the Commission has proposed a Directive concerning measures to ensure a high common level of network and information security across the Union (Network Information Security Directive)[10] with the following elements:

- Establishment of Computer Emergency Response Teams (CERTs): Member States are required to adopt a national strategy that sets out concrete policy and regulatory measures to maintain a level of network and information security. This includes designating a national competent authority for information security and setting up a CERT that is responsible for handling incidents and risks.
- Co-operation network: the competent authorities in EU Member States and the European Commission will form a co-operation network to co-ordinate against risks and incidents affecting network and information systems. The network will exchange information between authorities, provide early warnings on information security issues and agree on a co-ordinated response in accordance with an EU NIS co-operation plan.

[9] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667

[10] http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

- Security requirements: Member States must ensure that public and private sector take appropriate technical and organisational measures to manage the security risks to networks and ICT; these must guarantee a level of security appropriate to the risks and should prevent and minimise the impact of security incidents affecting the services they provide.
- Incident reporting: public and private sector must also notify the competent authority of incidents that have a significant impact on the continuity of these services. This is probably the most contentious item and both incident thresholds and the scope of public and private sector entities are still to be finalised. Where the security incident involves personal data, there may be a requirement to notify data protection authorities and individuals affected either existing EU data protection laws or the proposed EU data protection regulation which may be adopted in 2015 or thereafter.
- Use of standards: Member States are encouraged to use standards, such as ISO2700x series[11] for the implementation of security requirements.
- Enforcement: the competent authorities in each Member State are to be given powers to investigate cases of non-compliance of public bodies and market operators, which may include undergoing a security audit. They may also report criminal incidents to law enforcement authorities and work with data protection authorities where incidents involve personal data. The competent authorities and the single points of contact should be civilian bodies, subject to full democratic oversight and should not fulfil any tasks in the field of intelligence, law enforcement or defence or be organisationally linked in any wayto bodies active in those fields[12].
- The strategy also highlights the importance[13] of adhering to the protection of fundamental rights, freedom of expression, personal data and privacy as well as ensuring democratic and efficient multi-stakeholder governance.

2.1.2 European Network Information Security Agency (ENISA)

ENISA published 'An evaluation Framework for National Cybersecurity Strategies' in November 2014[14]. The Framework aims to evaluate cybersecurity strategies currently in place in eighteen European Union Member States. ENISA identified similarities between the different European strategies and their objectives; cybersecurity strategies often have objectives articulated around clusters (objectives), as does the European Cybersecurity Strategy[15]:

- To achieve cyber resilience: develop capabilities and cooperating efficiently within the public and private sector;
- To secure critical information infrastructures;
- To reduce cybercrime;
- To develop the industrial and technological resources for cybersecurity;
- To contribute to the establishment of an international cyberspace policy.

The Framework defines a set of key performance indicators (KPIs) to measure the effectiveness of a strategy. Examples of KPIs include the effective functioning of a CERT, a legislative framework, public-private cooperation, risk assessments for the national critical infrastructure, capacity building and the availability of a budget.

[11] http://www.27000.org/

[12] http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0244#def_1_2 (Amendment 11)

[13] http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security (pp 15, 16)

[14] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1/an-evaluation-framework-for-cyber-security-strategies/at_download/fullReport

[15] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

The European Union External Action Service (EEAS) also carried out activities related to cybercrime.[16]

2.1.3 Cybersecurity strategy of the United Kingdom

The cybersecurity strategy[17], issued in 2011, emphasises the role and responsibilities of civil society and industry in helping secure the UK against attacks. It also recognises that existing legislation and education at all levels should incorporate cybersecurity in their activities. Six central departments and nine other governmental organisations (including those in the Intelligence and Security Agencies) are responsible for delivery. The strategy sets out four key objectives:

- Tackle cybercrime and make the UK one of the most secure places in the world to do business in cyberspace;
- Be more resilient to cyberattacks and better able to protect UK's interests in cyberspace;
- Help shape an open, stable and vibrant cyberspace, which the UK public can use safely, and that supports open societies;
- Have the cross-cutting knowledge, skills and capability the UK needs to underpin all its cybersecurity objectives.

The UK published the 'ten steps to cybersecurity[18]', the cybersecurity information sharing partnership (CISP)[19] and the cyber essentials scheme[20], which promotes voluntary cyber certifications for businesses. The UK also launched its first national computer emergency response team, CERT-UK[21] which liaises with UK businesses and other CERTs – including those in financial services and education – on cybersecurity issues, and in particular those relating to national infrastructure.

2.1.4 Cybersecurity strategy of Estonia

The first Cyber Security Stratagy of Estonia 2008 – 2013 was one of the first such strategies in the world. The working groups to draft the strategy were established and work started in June 2007. Government adopted the strategy[22] in May 2008.

The strategy referred to the asymmetrical threats in cyberspace and considered the cyberattacks as serious security risks to the nation. Its purpose was to reduce the risks and vulnerabilities through national action plans and active international cooperation. It focused first on different principles to ensure cybersecurity, then analysed the threats in cyberspace and the fight against cybercrime, and explained different activities to support cyber security which included the legal framework, national and international frameworks and cooperation.

The strategic objectives were:

- The application of a graduated system of security measures in Estonia;
- The development of Estonia's expertise in and high awareness of information security to the highest standard of excellence;
- The development of an appropriate regulatory and legal framework to support the secure and seamless operationality of information systems;

16 http://eeas.europa.eu/enp/documents/progress-reports/index_en.htm

17 https://www.gov.uk/government/publications/cyber-security-strategy

18 http://www.cesg.gov.uk/News/Pages/10-Steps-to-Cyber-Security.aspx

19 https://www.cert.gov.uk/cisp/

20 https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

21 http://www.cesg.gov.uk/Pages/homepage.aspx

22 http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf

- The promotion of international co-operation aimed at strengthening global cyber security.

The strategy set out the following goals:

- The development and implementation of a system of security measures;
- The definition of Critical Infrastructure and the creation of necessary legal and organisational framework;
- The establishment of a Cyber Security Council under the Security Committee of the Government;
- The reorganisation of and empowering the Estonian Information System Authority with additional functions, including supervisory powers to increase competence and training;
- The development of a cyber security legal framework;
- The development and facilitation of international cooperation;
- The prevention and awareness raising of cyber security.

The strategy was accompanied by an action plan defining detailed goals and particular tasks to ministries and government institutions indicating deadlines and allocated resources. Encompassing civil, administrative, criminal and military aspects and legal frameworks, its holistic, interdisciplinary approach made it easier to plan and coordinate future activities, amendments to legislation to organisations and budgets.

The second Cybersecurity Strategy of Estonia[23] 2014 – 2017 is a follow-up to the previous strategy and has the mission to 'ensure national security and support the functioning of an open, inclusive and safe society' and cites the following subgoals:

- Ensuring the protection of information systems underlying important services;
- Enhancing of the fight against cybercrime;
- Development of national cyber defence capabilities;
- Estonia manages evolving cyber security threats;
- Estonia develops cross-sectoral activities.

Both 2008 and 2014 strategies are accompanied by a Strategy Action Plan which assigns tasks and roles. The Ministry of Economic Affairs and Communications directs cybersecurity policy and coordinates the implementation of the strategy. The strategy is implemented and assessed by all ministries and government agencies, especially the Ministry of Defence, the Information System Authority, the Ministry of Justice, Police and Border Guard Board, the Government Office, the Ministry of Foreign Affairs, the Ministry of the Interior and the Ministry of Education and Research, NGOs, business organisations, governments, and educational institutions in a cooperative and integrated manner. In 2009 a Cyber Security Council (CSC) was established under the Government Security Committee as a coordinating and advisory body, consisting of Deputy Permanent Secretaries from different ministries, plus representatives from other government institutions. If necessary, representatives of the private sector and academia are invited on ad hoc basis. Initially chaired by the Ministry of Defence, since 2011 this task was given to the Ministry of Economic Affairs and Communications. The CSC is also monitoring and assessing the implementation of the Action Plan

The Estonian strategy served as an example for Georgia as well as other States and is regarded as a good practice for a cybersecurity strategy within the wider Central and Eastern Europe region.

[23] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Estonia_Cyber_security_Strategy.pdf

2.1.5 Cybersecurity strategy of the Czech Republic

The Cybersecurity Strategy of the Czech Republic for 2011 – 2015[24] defines national interests and objectives, necessary to build up a credible information society with solid legal foundations, which is committed to a secure cyber transmission and processing of information in all domains of human activity and ensures that the information can be used and shared freely and safely. The following Strategic Objectives and Measures are outlined:

- Legislative Framework;
- Strengthening of Cybersecurity of Public Administration and Critical Infrastructure Information and Communication Systems and Technologies (CI ICTs);
- Establishment of a National CERT Agency;
- International Cooperation;
- Cooperation of the State, Private Sector and Academia;
- Increased Cybersecurity Awareness.

2.1.6 Cybersecurity Strategy of the Netherlands

While the Dutch approach reflects other international examples in its content[25], implementing a multistakeholder governance[26] approach is its priority objective. A National Cybersecurity Council, consisting of public sector entities (such as National Security, Ministry of Interior, and Telecommunications Agency), private sector entities (banks, ISP's, telecommunication providers, international software and hardware companies) and academics is an example of how the topic of cybersecurity is driven collaboratively, while respecting and observing each other's interests.

2.2 Developments in the area of cybercrime strategy/policy

Often, there is no distinct cybercrime strategy or policy in place. However, elements can be found in Cybersecurity and Serious Organized Crime Strategies, as the UK example demonstrates.

2.2.1 Cybercrime strategy of the UK

In March 2010, the UK launched its Cybercrime Strategy[27], outlining definitions of cybercrime (financially-based crimes such as fraud, identity theft, and intellectual property theft as well as non-financial crimes such as threats to children, hate crimes, harassment, and political extremism), the parties involved and the approach to tackling cybercrime.

This strategy was superseded in 2011 by the revised Cybersecurity Strategy, incorporating both cybersecurity and cybercrime aspects[28].

As a result, the government launched the National Crime Agency ('NCA') in October 2013, which includes a new national cybercrime unit (NCCU)[29,] bringing together specialists from the Police Central e-Crime Unit in the Metropolitan Police Service and the former Serious Organised Cime

[24] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/CzechRepublic_Cyber_Security_Strategy.pdf

[25] http://english.nctv.nl/Images/national-cyber-security-strategy-2_tcm92-520278.pdf

[26] http://www.infosecisland.com/blogview/14968-Dutch-Cyber-Security-Council-Now-Operational.html

[27] https://www.gov.uk/government/publications/cyber-crime-strategy

[28] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_cy_strats_rep_V23_30march12.pdf

[29] https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace/supporting-pages/setting-up-a-national-cyber-crime-unit

Agency Cyber to create technical, tactical intelligence and investigations expert teams[30]. Besides this new agency, the government launched its Serious and Organised Crime Strategy[31].

The National Crime Agency distinguishes between consumer and business-related threats. Regarding consumer related threats, the NCA outlines that organized crime has been quick to take advantage of the opportunities offered by the Internet, particularly of the growth in e-commerce and online banking. It warns of specialist criminal groups targeting individuals, small businesses and large corporate networks to steal personal information in bulk in order to profit from the breached data available to them. The most common consumer-related threats are phishing, webcam hijacking, file hijacking, keylogging, screen shots and ad clicking.

2.2.2 Good practice study on cybercrime reporting mechanisms

In September 2014, the Council of Europe published a *Good practice study on cybercrime reporting mechanisms*[32]. Building on the experience of several existing reporting mechanisms from both public and private sectors around the world (Belgium, EU, France, Mauritius, Netherlands, UK, USA), it aims at providing advice to countries which are considering or are in the process of setting up their own cybercrime reporting mechanisms.

The recommendations provided in this study are relevant for cybersecurity strategies as cybercrime reporting mechanisms contribute to identifying trends and fostering cooperation and information sharing. Besides their diversity, cybercrime reporting mechanisms share the fact that they make a positive contribution to the fight against cybercrime, in particular in the following aspects:

- Providing actionable information/complaints which can be the basis for investigations and prosecutions;
- Identification of cybercrime threats on citizens and organisations;
- Understanding and measuring trends;
- Establishing a channel of communication between citizens (victims/witnesses of cybercrime) and the authorities/initiatives in charge;
- Coordination between law enforcement and public authorities;
- Fostering a culture of public/private cooperation and information sharing.

2.3 Selection of assessment criteria based on current developments

2.3.1 Assessment criteria for a cybersecurity strategy

Analyzing examples from UK, Czech Republic, Estonia, ENISA and the EU NIS Directive, supporting measures are identified that will be used to assess the current status of EAP country strategies. These developments include:

- Cybersecurity strategy identification of cybercrime prevention as a key objective
- Establishment of computer emergency response teams (CERTs);
- Cooperation on both national and international levels;
- Cooperation with private sector;
- Multi-stakeholder governance;
- Support of economic growth;
- Mandating minimal technical safeguards;

[30] http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit

[31] https://www.gov.uk/government/publications/serious-organised-crime-strategy

[32] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/GLACY/Reports/2688_6_4_GLACY_study_Rep_Mechanisms_v5_ENG.pdf

- Reporting mechanisms;
- Education and capacity building;
- Protecting fundamental rights, freedom of expression, personal data and privacy;
- Follow-up to strategy and action plans (evidence of country ownership)

2.3.2 Assessment criteria for a cybercrime strategy

The developments in the UK are in many ways representative of the approach chosen by many countries and institutions listed in the section 'International Developments': the issue of cybersecurity and cybercrime is addressed in one single, holistic strategy aiming at directing government's resources and activities in an integrated policy.

Elements of a cybercrime strategy – or more precisely of a strategy on cybercrime and electronic evidence – may comprise:[33]

- Cybercrime reporting mechanisms;
- Prevention;
- Legislation, incl. safeguards and data protection
- Specialised units;
- Interagency cooperation;
- Law enforcement training;
- Judicial training;
- Public/private cooperation;
- Effective international cooperation;
- Financial investigations and prevention and control of fraud, money laundering and terrorist financing;
- Specific measures for the protection of children online.

These elements are also largely reflected in the Strategic Priorities adopted in Kyiv meeting under the CyberCrime@EAP project in October 2013[34].

For the purposes of the present report, the assessment will primarily focus on:

- Public/private cooperation in particular cooperation between law enforcement authorities and Internet Services Providers (ISPs), CERTs;
- International cooperation;
- Establishment of platforms for reporting on cybercrime.

2.3.3 Assessment summary structure

The EAP country strategies will be assessed according to the following structure. In the remainder of the report below, sections x.1 and x.2 provide a brief narrative overview of the country situation. In section x.3 a brief overview in table format is given as a summary overview. Where no official cybersecurity or cybercrime strategy is available, the assessment is based on information provided or, where specified, on public information.

[33] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_cy_strats_rep_V23_30march12.pdf

[34] as outlined in the Strategic Priorities for the Cooperation against Cybercrime in the Eastern Partnership Region (Kyiv, Ukraine, 31 October 2013)

Assessment structure

Cybersecurity	
Cybersecurity strategy in place	Yes/no/remarks
Cybersecurity strategy names preventing cybercrime as a key objective	Yes/no/remarks
Establishment of computer emergency response team(s), CERTs	Yes/no/remarks
Cooperation on both national and international level;	Yes/no/remarks
Cooperation with private sector	Yes/no/remarks
Multi-stakeholder governance	Yes/no/remarks
Support of economic growth	Yes/no/remarks
Mandating minimal technical safeguards	Yes/no/remarks
Reporting mechanism	Yes/no/remarks
Education and capacity building	Yes/no/remarks
Protecting fundamental rights, freedom of expression, personal data and privacy	Yes/no/remarks
Cybercrime	
Cybercrime strategy in place	Yes/no/remarks
Public/private cooperation	Yes/no/remarks
International cooperation	Yes/no/remarks
Establishment of platforms for reporting cybercrime	Yes/no/remarks

3 Armenia

3.1 Cybersecurity strategy

Armenia has been subject to cyber-attacks in the past, such as a number of Distributed Denial of Service (DDoS) attacks in 2013 and 2014[35].

Armenia identified the following cyber-threats as prevalent[36]:

- Hacking attacks on websites and other resources in the Armenian segment of the Internet;
- Embezzlement and distribution of personal data;
- Development, use and distribution of malware;
- Distribution of pornography in the Internet;
- Misappropriation of computer data;
- Fraud by means of computer devices;
- Illegal enterprises providing telecommunications services.

Although Armenia has not published a formal cybersecurity strategy, the National Security Service (NSS) is responsible for cybersecurity policy[37] and the protection of government websites and networks. Furthermore, a concept for an Information Security Strategy[38] was developed in 2009, which outlines certain activities to be implemented. In addition, during the meeting in Chinisau, the Armenian representative mentioned that the Digital Society 2020 Strategy includes certain measures regarding cybersecurity activities and laws in the area of cybersecurity and data protection, currently under discussion.

The OSCE (Organisation of Security and Cooperation in Europe) has organised several capacity-building activities for Armenia in 2014, including:

- Visit by the OSCE to the Ministry of Defense (14 November 2014)[39];
- Cybercrime training for Armenia and Georgia (26-27 November)[40].

The OSCE Strategic Framework for Police (2012) sets two objectives related to cybercrime strategies (§19):

- Facilitate, at the regional and national levels, capacity-building and the exchange of information and best practices in investigating cybercrime and dealing with cyber evidence, with a special focus on fighting hate speech[41] and the sexual exploitation of children on the Internet as well as countering the use of the Internet for terrorist purposes in conformity with human rights, fundamental freedoms and the rule of law;
- Assist the participating States in reaching the level of technical expertise required to join the G8 24/7 cybercrime network

[35] http://noravank.am/arm/articles/security/detail.php?ELEMENT_ID=12706

[36] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_Project_EaP/Chisinau_International_Conference_Nov2014/CyberEAP%20AssessRep_v15.pdf

[37] http://armenpress.am/eng/news/633325/www.idealsystem.am

[38] Source: Mediamax, Armenia, April 30 2009

[39] http://www.aysor.am/en/news/2014/11/14/mod-davit-tonoyan/871978

[40] http://www.osce.org/secretariat/127361

[41] http://www.osce.org/fom/106289

3.1.1 CERT

An active CERT is listed[42], however, the CERT is not a FIRST member and the website[43] appears to be out of service.

3.2 Cybercrime strategy

No information regarding a cybercrime strategy has been received.

3.2.1 International cooperation

The COE EAP Assessment report on Criminal justice capacities on cybercrime and electronic evidence in the Eastern Partnership region, results of the peer-to-peer assessments under the CyberCrime@EAP project states[44] the following in section 2.4:

- Mutual legal assistance requests are governed by article 499-6 of the Criminal Procedure Code. The competent authority is the General Prosecutor's Office.
- Police-to-police cooperation is conducted by 24/7 networks. The 24/7 contact point is established within the Division for Fighting against High Tech Crimes, and has no competence to send or receive mutual assistance requests.
- In the area of mutual assistance requests, Armenia cooperates actively with the OSCE office in Yerevan as well as the US Embassy, which formally assisted the country and provided equipment.

Armenia is a Party to the Budapest Convention on Cybercrime and participated in the assessment of the mutual legal assistance provisions of this treaty in 2013 and 2014. The recommendations adopted by the Cybercrime Convention Committee also apply to Armenia[45].

3.2.2 Reporting mechanism

No specific contact points have been designated by law enforcement and ISPs for their communications. Reportedly, cooperation arrangements are in place between the State Security Service and the Internet community, although no details were provided.

3.2.3 Public/private cooperation

Collaboration with public sector in general and specifically with ISPs based on the 'Guidelines for Cooperation between Law Enforcement and Internet Service Providers against Cybercrime' developed by the Council of Europe is reportedly ongoing.[46] The COE EAP Assessment report suggests the continuation of these efforts and refers to the Georgian model[47].

[42] http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

[43] www.cert.am

[44] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_Project_EaP/Chisinau_International_Conference_Nov2014/CyberEAP%20AssessRep_v15.pdf

[45] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf

[46] ibid. 2.7.2

[47] Ibid. 2.10

3.3 Armenia summary

Assessment item	Republic of Armenia
Cybersecurity	
Cybersecurity strategy in place	In concept stage
Cybersecurity strategy names preventing cybercrime as a key objective	n/a
Establishment of computer emergency response team(s), CERTs	Yes
Cooperation on both national and international level;	n/a
Protecting fundamental rights, freedom of expression, personal data and privacy.	n/a
Cooperation with private sector	n/a
Multi-stakeholder governance	n/a
Support of economic growth	n/a
Mandating minimal technical safeguards	n/a
Reporting mechanism	n/a
Education and capacity building	n/a
Protecting fundamental rights, freedom of expression, personal data and privacy	n/a
Cybercrime	
Cybercrime strategy in place	No information
Public/private cooperation	supported by CoE EAP project 2011-14 and recommended to be continued
International cooperation	supported by CoE EAP project 2011-14 and recommended to be continued
Establishment of platforms for reporting cybercrime	supported by CoE EAP project 2011-14 and recommended to be continued

4 Azerbaijan

4.1 Cybersecurity strategy

No information was transmitted by national authorities regarding the existence or/preparation of a cybersecurity strategy. However, Azerbaijan has an information society strategy, which encompasses most aspects of a cybersecurity strategy ('National Strategy of the Republic of Azerbaijan on the Development of the İnformation Society for the period 2014 -2020'[48]).

The main objective of the National Strategy is the establishment of a national information society in the country to:

- Ensure that the growing demand for information and telecommunications infrastructure modernisation is met, provision of quality services to people, businesses and society as a whole, expanding the use of information and technology;
- Improve the quality of ICT services provided;
- Support the implementation of effective regulation of the information society, including respecting human rights, especially the rights of every individual to communicate information and to have comprehensive and free access to information on the internet.
- Enable the establishment of a competitive and export-oriented ICT industry, by introducing a new type of economy, to ensure the transition to knowledge-based economy;
- Establish 'E-government' by the use of ICT to enhance and improve the efficiency of public administration, the development of democratic principles and achieve high quality of e-services;
- Foster information and telecommunication technologies in the field of high-level scientific and skilled personnel;
- Support ICT for every citizen to receive education and training opportunities, information and culture to improve the safe use of ICT;
- Support the protection of national interests in the world media, legal and safe use of ICT in society, modern technologies in order to increase confidence in the development of information security systems.

The State Agency for Special Communications and Information Security and the Electronic Security Centre has recently started activities to enhance Azerbaijan's information security, in particular by strengthening the information systems of State bodies and raising awareness of cyberthreats among the population.

4.1.1 CERT

Azerbaijan has a national CERT: AZ-CERT, under the responsibility of the Ministry of Communications and High Technologies.

4.1.2 International Cooperation

International cooperation in the field of ICT to expand bilateral and multilateral cooperation is specifically mentioned as one of the main goals of the strategy. Azerbaijan has official partnerships with Russia, Ukraine, Republic of Latvia, Republic of Slovakia and Japan to share information on cyber threats.

[48] http://president.az/articles/11312

4.1.3 Public/private cooperation

Cooperation with private sector and civil society institutions is mentioned in the 'National Strategy of the Republic of Azerbaijan on the Development of the İnformation Society for the period 2014 - 2020'. Also, the public sector is enabled to foster information sharing on the cybersecurity environment and assess the implementation status of the National Strategy.

4.1.4 Multi-stakeholder governance

The strategy identifies civil society institutions and the public sector as stakeholders and outlines the importance of giving regular updates to the public on the implementation of the National Strategy.

4.1.5 Supporting economic growth

Another key element of the national strategy is the development of an ICT sector in order to foster economic growth, lessen the dependency on the oil sector and promote a knowledge-driven society.

4.1.6 Mandating minimal technical standards

While not specifically mentioned in the national strategy, the Standards, Metrology and Patents Committee of Azerbaijan[49] has the mandate to implement internationally recognized cybersecurity standards across sectors.

4.1.7 Education and capacity building

The Ministry of Communication and High Technologies of Azerbaijan has established research and development programs in the area of cybersecurity standards, best practices and guidelines, appilicable both to the private and public sector. As part of the National Strategy, Azerbaijan plans to hold training courses on e-Government and information security, while the AZ-CERT further supports capacity building in the technology domain.

4.1.8 Protecting fundamental rights

The strategy stresses the need to support freedom of expression on the Internet and public access to information.

4.2 Cybercrime strategy

There is no information available on a specific cybercrime strategy.

4.2.1 International Cooperation

The Azerbaijani Centre of Electronic Safety under the Communications and High Technologies Ministry has become a member of the Anti-Phishing Working Group (APWG).[50]

Azerbaijan is a Party to the Budapest Convention on Cybercrime and participated in the assessment of the mutual legal assistance provisions of this treaty in 2013 and 2014. The recommendations adopted by the Cybercrime Convention Committee also apply to Azerbaijan[51].

[49] http://www.azstand.gov.az

[50] http://www.azernews.az/business/68695.html

[51] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf

4.2.2 Public/private cooperation

No information available.

4.2.3 Reporting mechanism

No information available.

4.3 Azerbaijan summary

Assessment item	**Republic of Azerbaijan**
Cybersecurity	
Cybersecurity strategy in place	Yes, National strategy on the information society contains all elements but is not named cybersecurity strategy.
Cybersecurity strategy mentions the prevention of cybercrime as a key objective	No
Establishment of computer emergency response team(s), CERTs	Yes
Cooperation on both national and international level;	Yes
Cooperation with private sector	Yes
Multi-stakeholder governance	Yes
Support of economic growth	Yes
Mandating minimal technical safeguards	Yes
Reporting mechanism	No
Education and capacity building	Yes
Protecting fundamental rights, freedom of expression, personal data and privacy	Yes
Cybercrime	
Cybercrime strategy in place	No information
Public/private cooperation	No information
International cooperation	Yes
Establishment of platforms for reporting cybercrime	No information

5 Republic of Belarus

5.1 Cybersecurity strategy

Belarus National Security Concept of 2010[52] is based on a threat assessment, which identifies the following challenges:

- Rise of crime using ICT technology;
- Unauthorised access from outside to the information resources of Belarus that harm its national interests;
- Insufficient safety arrangements protecting the vital information facilities.
- The overall number of computer related crimes registered is increasing.

Embezzlement via computer systems is the most common form of cybercrime committed in Belarus (approx. 90% of cybercrime offences). This form of crime –1,000 to 1,500 per year on average – is expected to keep rising in the next years.

Unauthorised access, alteration or misappropriation of computer data as well as distribution of malware amount to 3% and 1% respectively of the total cybercrime offences. So-called telecom crimes (e.g. roaming fraud, illegal provision of telecom services) are currently not a widespread phenomenon.

As regards acts against national interests, the Ministry of State Security reported that attacks against government institutions and activities of cyber-espionage are severely affecting Belarus.[53]

As per information received by the Belarus delegation following the Chinisau event, there is no cybersecurity or cybercrime strategy available for now in Belarus. However, a number of legal acts regulate elements of cybersecurity and cybercrime:

- The Constitution of the Republic of Belarus of 1994 (as amended, adopted at the national referenda on 24 November 1996 and 17 October 2004)[54]
- Act of November 10, 2008 № 455-Z 'On Information and Protection of Information'55
- Presidential Decree dated February 1, 2010 № 60 'On Measures to Improve the Use of the National Segment of the Internet»[56]
- The National Security Concept of the Republic of Belarus, approved by Decree of the President of 09.11.2010 № 57557, defines information security as a condition to protect the balanced interests of the individual, society and the State from external and internal threats in the information sphere and identifies it as an independent component of national security
- The Criminal Code 1999[58] identifies articles 212, 349-355, 201, 222, 343, 343-1 (relating to crimes against information security, Internet, various instruments of electronic payment systems, counterfeit means of payment).
- The Code of Administrative Offences[59]

---

[52] Presentation at Chinisau by Review of Cybercrime@EAP, Republic of Belarus Investigative Committee , Aleksandr SUSHKO

[53] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_Project_EaP/Chisinau_International_Conference_Nov2014/CyberEAP%20AssessRep_v15.pdf

[54] http://etalonline.by/Default.aspx?type=text&regnum=v19402875#load_text_none_2_

[55] http://etalonline.by/Default.aspx?type=text&regnum=H10800455#load_text_none_1_

[56] http://www.etalonline.by/Default.aspx?type=text&regnum=P31000060#load_text_none_1_1

[57] http://pravo.by/world_of_law/text.asp?RN=P31000575

[58] http://etalonline.by/?type=text&regnum=HK9900275#load_text_none_1_

[59] http://etalonline.by/?type=text&regnum=Hk0300194#load_text_none_1_

- The State program to combat human trafficking, illegal migration and related wrongful acts for 2012-2013, approved by Presidential Decree of 02.10.2010 №518, which provides for the possibility to join the Council of Europe's Convention on Cybercrime of 23 November 2001.
- The strategy for Information Society Development in the Republic of Belarus for the period up to 2015 approved by the Council of Ministers of 09.08.2010 № 1174[60].
- This strategy was developed under the national program of accelerated services development in the field of information and communication technologies 2011-2015.[61] Its purpose is to create conditions for the accelerated development of IT services; promote the development of information society on the basis of innovation; and improve the quality and efficiency of information for the population, business and government. One of its 9 sub-programs focuses on 'security of ICT and digital trust'.
- The Ministry of Communications and Information has initiated the development of the Information Society Development Strategy of the Republic of Belarus for 2016-2020.
- Presidential Decree of November 8, 2011 № 51562 on Information security issues.

5.1.1 CERT

Belarus has a national CERT: CERT-BY. The main task of the Centre is to reduce threats to information security within Belarus[63].

5.1.2 Public/private cooperation

The National Programme[64] was jointly developed by the public and private sector. The national programme consists of nine subprograms under the responsibility of different public sector agencies[65]:

- 'National Information and Communication Infrastructure' - Ministry of Communications and Information;
- 'The development of export-oriented IT industry' - State Institution 'Administration of High Technologies Park';
- 'Electronic Government' - Department of Information Ministry of Communications;
- 'E-health' - Ministry of Health;
- 'E-employment and social protection of the population' - Ministry of Labor and Social Protection;
- 'E-learning and the development of human capital' - Ministry of Education;
- 'The formation of national content' - Ministry of Information;
- 'Electronic Customs' - State Customs Committee;
- 'Security of information and communication technologies and digital trust' - Department of the Ministry of Communications and Information Operations and Analysis Centre under the President.

[60] http://e-gov.by/zakony-i-dokumenty/programma-elektronnaya-belarus/strategiya-razvitiya-informacionnogo-obshhestva-v-respublike-belarus-na-period-do-2015-goda

[61] http://e-gov.by/zakony-i-dokumenty/programma-elektronnaya-belarus/nacionalnaya-programma-uskorennogo-razvitiya-uslug-v-sfere-informacionno-kommunikacionnyx-texnologij-na-20112015-gody

[62] http://e-gov.by/zakony-i-dokumenty/zakony-ob-obrashheniyax-grazhdan/o-nekotoryx-voprosax-razvitiya-informacionnogo-obshhestva-v-respublike-belarus

[63] https://cert.by/

[64] http://e-gov.by/zakony-i-dokumenty/programma-elektronnaya-belarus/nacionalnaya-programma-uskorennogo-razvitiya-uslug-v-sfere-informacionno-kommunikacionnyx-texnologij-na-20112015-gody

[65] ibid.

5.2 Cybercrime strategy

There is no specific cybercrime strategy available.

5.2.1 International cooperation

International cooperation is regulated by section XV of the Criminal Code. When foreign cooperation is required, the department forn investigation of crimes against information security and intellectual property of the Main Investigative Department of the Investigative Committee of the Republic of Belarus sends a mutual assistance request through the General Prosecutor's Office to the LEA of the requesting state. While the Ministry of Justice signs MLAT agreements, the Investigative Committee is competent for mutual legal assistance applications. Participation in the Budapest Convention would enable legal assistance in criminal matters, provide information exchange and cooperation with law enforcement authorities of States Parties in the fight against cybercrime.

The contact point is established in the Ministry of Interior's 'K' Department. Since 2008, Belarus belongs to the international network of contact points established under the G8 Rome–Lyon Group. The resources of the national bureau of Interpol in Belarus are often used as well. The 'K' Department also cooperates with foreign LEA in the form of joint international operations against cybercrime, in particular in the field of child pornography and bankcard fraud. Police-to- police cooperation is possible, but the daily practice of Law Enforcement Agencies was not described in sufficient detail for an assessment to be made[66].

5.2.2 Public/private cooperation

Enhancing collaboration with the public sector in general and more specifically with ISPs, based on the Council of Europe's 'Guidelines for Cooperation between Law Enforcement and Internet Service Providers against Cybercrime' remains 'not completed'.[67]

5.2.3 Reporting mechanism

No information available.

[66] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_Project_EaP/Chisinau_International_Conference_Nov2014/CyberEAP%20AssessRep_v15.pdf 3.41

[67] ibid. 3.9

5.3 Belarus summary

Assessment item	Belarus
Cybersecurity	
Cybersecurity strategy in place	No
Cybersecurity strategy names preventing cybercrime as a key objective	No
Establishment of computer emergency response team(s), CERTs	Yes
Cooperation on both national and international level;	Yes, on national level
Cooperation with private sector	Yes
Multi-stakeholder governance	No information
Support of economic growth	Yes
Mandating minimal technical safeguards	No information
Reporting mechanism	No information
Education and capacity building	Yes
Protecting fundamental rights, freedom of expression, personal data and privacy	Yes
Cybercrime	
Cybercrime strategy in place	No
Public/private cooperation	supported by CoE EAP project 2011-14 and recommended to be continued
International cooperation	supported by CoE EAP project 2011-14 and recommended to be continued
Establishment of platforms for reporting cybercrime	supported by CoE EAP project 2011-14 and recommended to be continued

6 Georgia

6.1 Cybersecurity strategy

Georgia has been subject to a number of cyber attacks in the past years. The cybersecurity strategy lists the following primary threats to the Georgian critical infrastructure:

- Cyber conflict: In 2008, in parallel to a military conflict, Georgia was subject to cyber attacks, in a demonstration of Georgia's vulnerability to potential adversaries possessing advanced capabilities for cyberwar.
- Cyber terrorism: The growing dependence of Georgian state management and business on critical information systems has led to elevated cyber terrorism threats.
- Cybercrime and other security threats: Security challenges for Georgia include categories of cyber offences directed against critical information systems, to obtain secret information, to conduct economic sabotage and for other politically motivated aims, as well as lesser acts against information/cybersecurity jeopardising access to information/operation of information systems.

As a result, a cybersecurity strategy working group, the 'Permanent Inter-agency Commission', under the auspices of the National Security Council, has developed a Georgian National Cybersecurity Strategy 2012-2015[68], reflecting strategic goals and guiding principles, defining action plans. The Strategy outlines three major goals:

- Uniform government approach;
- Public-private cooperation;
- Active international cooperation.

Based on this Strategy, the Government undertakes actions to facilitate the safe operation of State agencies, private sector entities and public users in cyberspace, and to secure electronic transactions and the unhindered functioning of Georgian economy and business.

The Cybersecurity Strategy is part of the overall package of conceptual and strategic documents developed in the framework of the National Security Review process, such as the Threat Assessment Document for 2010-2013[69] and the National Security Concept of Georgia[70]. Currently, the Office of State Security and Crisis Management Council is elaborating a draft Threat Assesment document that reflects all possible threats, risks and challenges (including cyber threats) to Georgian national security. Once the Threat Assessment document is approved by the Government, all relevant cybersecurity related conceptual documents including the Cyber Security Strategy as well as legal texts will be revised and updated in accordance with the new security environment. The Council of Europe Cybercrime Convention Committee will be actively involved in this process,

In the wake of the 2008 conflict, Georgia has accorded high priority to cyber defence issues. Hence, in March 2014 the Ministry of Defence established the Cybersecurity Bureau. The remit of the new Bureau is to establish and enhance secure and credible ICT infrastructure capabilities for the Defence Sector. The Cyber Defence Policy was drafted by the Cybersecurity bureau in consultation with NGOs and NATO and other partners. Now that the policy document has been adopted, the Bureau is preparing a Cyber Defence Development Strategy

[68] http://www.dea.gov.ge/uploads/National%20Cyber%20Security%20Strategy%20of%20Georgia_ENG.pdf

[69] http://www.jamestown.org/programs/edm/single/?tx_ttnews%5Btt_news%5D=37077&cHash=b5f134057b#.VM-0Gul0yUk

[70] http://gfsis.org/media/download/GSAC/resources/National_Security_Concept_Georgia.pdf

6.1.1 CERT

There are two active CERTs listed[71]:

- CERT-GE[72]: Research and Education CERT;
- CERT-GOV-GE[73]: Government CERT.

6.1.2 International Cooperation

The strategy mentions the following cooperation models:

- Strengthening relations in cybersecurity matters with international organisations working in the field of cybersecurity (OECD, EU, OSCE, NATO, UN, ITU) as well as relevant national authorities;
- Active participation in international activities related to cybersecurity and supporting relevant initiatives on a regional scale;
- Initiating bilateral and multilateral cooperation with national CERTs in the area of cybersecurity.

6.1.3 Public/private cooperation

The development of mechanisms for cooperation extending beyond governmental agencies to public-private partnerships is essential for ensuring the successful implementation of a cybersecurity strategy. The cybersecurity strategy mentions that a larger part of the critical information systems of Georgia is owned by private businesses. Consequently, relevant experience and knowledge is mainly available in private companies.

6.1.4 Multi-stakeholder governance

The Strategy outlines roles and responsibilities within the public sector for the Data Exchange Agency, Ministry of Justice, Ministry of Education and Science, Ministry of Foreign Affairs, CERT-GOV-GE, and the National Security Council. Pursuant to the 2014 Constitutional amendments, responsibility for cybersecurity (along with other national security functions) has been vested in the Government. The Multi Stakeholder Governence process will now be coordinated by the Prime-Minister's Advisory body, the State Security and Crisis Management Council.

6.1.5 Support of economic growth

The introductory section of the strategy provides that 'the Government of Georgia will undertake actions facilitating the safe operation of State agencies, the private sector and the public in cyberspace, secure electronic transactions and the unhindered functioning of Georgian economy and business.'

6.1.6 Mandating minimal technical safeguards

The Law of Georgia on Information Security[74], section 6, provides:

> 'Based on the consent of the critical information system subject, the Data Exchange Agency or a person or organisation selected by the critical information system from the pool of organisations or persons duly authorized by the Data Exchange Agency, the subject shall conduct an assessment of compliance of the information security policy of the critical information

[71] http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

[72] http://grena.ge/eng/services/cert

[73] http://www.dea.gov.ge/

[74] http://dea.gov.ge/uploads/InfoSec%20Law%20ENG.pdf

system subject according to minimum security standards set by the Data Exchange Agency (information security audit). The audit report created as a result is subject to obligatory implementation.'

6.1.7 Reporting mechanism

Georgia has a Law of Georgia on Information Security[75] which names the national CERT as the unit to which cyber incidents within Critical Infrastructure must be reported (Article 10).

6.1.8 Education and capacity building

The cybersecurity strategy outlines a number of initiatives to raise public awareness and set up educational programs, such as:

- Training of staff and technical personnel dealing with critical information systems about international and local standards of information security;
- Training of specialised cybercrime experts in the area of handling electronic evidence (cyber forensics);
- Support science and research projects in cybersecurity;
- Creation of a research lab.

6.1.9 Protecting fundamental rights

The National Security Concept recognises that 'the rights and freedoms of the Universal Declaration of Human Rights, the UN Convention on Civil and Political Rights, and the European Convention on Human Rights and Fundamental Freedoms are recognized by Georgia and guaranteed by its Constitution. Georgia guarantees the rights and freedoms of all citizens and groups residing in Georgia, respects their right of free choice, guarantees the right to freedom of speech, thought, conscience, religion, and belief, and creates a favorable environment that enables each citizen to realize his or her potential'. Newly enacted ammendements to the Criminal Procedure Code exclude cyber intrusive measures for minor crimes, restricting cyber interceptions to grave and exceptionally grave crimes, in conformity with ECHR standards.

6.2 Cybercrime strategy

Cybercrime is specifically addressed in the Cybersecurity Strategy of Georgia (section 4.2.):

- Introduction of the legal basis for Computer Emergency Response Team operations;
- Ratification of the 2001 Council of Europe Convention Against Cybercrime[76];
- Identification of an agency or agencies responsible for information security policies and coordination;

Although Georgia lacks a dedicated cybercrime strategy, save in the more general context of cybersecurity as just noted, its Organized Crime Strategy (2013 – 2014) specifically addresses cybercrime (chapter III)[77]:

- Counter-cybercrime directions and priorities;
- Capacity building of cyber law enforcement staff as top priority in process of combatting cybercrime;
- Adoption of the strategy positively assessed by the relevant national and international stakeholders.

[75] http://dea.gov.ge/uploads/InfoSec%20Law%20ENG.pdf

[76] 6/6/2012

[77] Presentation by the Georgian delegation (David Gabekhadze)

Standard Operational Procedures on initial handling and further forensics of digital evidence have been prepared based on T-CY Guidelines.

6.2.1 International cooperation

In October 2013, the National Assembly of Georgia approved a law on international police cooperation that provides for the possibility of cooperation specifically pursuant to the Budapest Convention. It addresses police-to-police cooperation and allows LEA of Georgia to undertake enforcement operations with foreign LEAs or international institutions – even in the absence of a formal agreement.[78]

Georgia is a Party to the Budapest Convention on Cybercrime and participated in the assessment of the mutual legal assistance provisions of this treaty in 2013 and 2014. The recommendations adopted by the Cybercrime Convention Committee also apply to Georgia[79].

6.2.2 Public/private cooperation

A Memorandum of Understanding for LEA/ISP cooperation has been adopted. The Memorandum aims at the effective cooperation of LEA and ISPs in the investigation of cybercrime, while at the same time protecting the right to privacy. It sets out basic rights and responsibilities of both stakeholders, including the obligation of LEAs to provide as much information as possible about the investigation without prejudice to interests at stake, such as confidentiality, etc.[80]

6.2.3 Reporting mechanism

Fullfilment of the tasks and the goals set forth in the Cybercrime Strategy and Action Plan (Organized Crime Strategy, III Chapter) is overseen by the Council for Combatting Organized Crime. The Council will launch a renewal process for the Strategy this year in which the CoE Cybercrime Convention Committee will be actively involved.

[78] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_Project_EaP/Chisinau_International_Conference_Nov2014/CyberEAP%20AssessRep_v15.pdf

[79] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf

[80] ibid.

6.3 Georgia summary

Assessment item	Georgia
Cybersecurity	
Cybersecurity strategy in place	Yes
Cybersecurity strategy names preventing cybercrime as a key objective	Yes
Establishment of computer emergency response team(s), CERTs	Yes
Cooperation on both national and international level;	Yes
Cooperation with private sector	Yes
Multi-stakeholder governance	Yes, within public sector
Support of economic growth	Yes
Mandating minimal technical safeguards	Yes
Reporting mechanism	Yes
Education and capacity building	Yes
Protecting fundamental rights, freedom of expression, personal data and privacy	Yes
Cybercrime	
Cybercrime strategy in place	Organized crime strategy in place, in addition to cybercrime mentioned as one of the priorities in the cybersecurity strategy
Public/private cooperation	Yes, with ISP
International cooperation	Yes
Establishment of platforms for reporting cybercrime	supported by CoE EAP project 2011-2014 and recommended to be continued

7 Republic of Moldova

7.1 Cybersecurity strategy

Moldova is currently drafting its cybersecurity strategy. However, during the presentation in Chinisau, the Moldovan delegation mentioned that Government authorities do not consider cybersecurity to a sufficient degree: when creating and deploying IT systems, most businesses, companies and public administration do not pay attention to the issues of cybersecurity assurance. Legislation in the field of information and communication technology is insufficiently harmonized and adapted. The Intelligence and Security Service has assumed the role of drafting and implemention of the cybersecurity policy[81] .

The delegation also mentioned the lack of state institutions directly accountable for coordinating and directing legislative activities in cybersecurity and inefficient or non-existent collaboration between institutions involved in cybersecurity.

According to the above-mentioned presentation, the draft National Security Strategy states in Section 4.7: 'Regarding information security, state authorized institutions will have an increasing role to ensure secure and efficient management of national information systems, both at the legal and functional levels by reducing the main risks, which are: network attacks (cyber-crimes), computer viruses, software vulnerability, negligence or malevolent users connected to unauthorized third parties. In this regard, the relevant regulatory framework will be adjusted to establish an effective mechanism for monitoring, control and implementation in order to reduce existing disparities and challenges, and with the aim of protecting society from possible attempts regarding misinformation and/or manipulating information from outside. Civil society will be consulted in this process.

By decision No 01/1-02-05 of 7 October 2014, the Supreme Security Council recommended to the Moldovan government that it[82:]

- Ensures the enforcement of the action plan on the implementation of the National Strategy for Information Society Development, Digital Moldova 2020, approved under the Government Decision No 857 of 31 October 2013;
- Ensures the creation of the national centre for reaction to security incidents (CERT), which in addition to essential duties, will define a joint instrument in carrying out public campaigns to inform the State, companies and citizens about digital crimes, threats and ways of preventing them;
- Ensures the drafting and promotion of draft legislative acts concerning information security, preventing and combating information and telecommunication offences (including a draft law on the amendment and completion of legislative acts, adopted by the cabinet under the Decision No 784 from 25 September 2014), and which aim at ensuring the management of national information security, in compliance with international standards;
- Ensures the elaboration, approval and implementation of a series of proactive and reactive measures to reduce possible information threats, mitigate the impact of information attacks and incidents coming from the cybernetic space;
- Ensures the further development of the special governmental system of telecommunications of the public administration authorities (protected governmental data transfer network) throughout the territory of Moldova;
- Ensures the establishment and approval of a national programme for continuous education of civil servants, private sector employees and citizens on possible cybernetic

[81] http://www.sis.md/en/ensuring-informational-security

[82]http://www.presedinte.md/eng/comunicate-de-presa/consiliul-suprem-de-securitate-a-examinat-chestiuni-legate-de-securitatea-informationala-a-republicii-moldova

risks and dangers resulting from the improper use of applications, information technologies and electronic communications, as well as about the negative consequences of cybernetic attacks;
- Ensures the drafting and approval of a draft law on ratification of the additional protocol to the Council of Europe Convention on Cybercrime[83].

7.1.1 CERT

Two CERTs have been established for Moldova:

- CERT Moldova[84] is the national CERT located at the RENAM, Research and Education National Association of Moldova.
- In accordance with Government Decision no. 746/2010, a Centre for Cyber Cecurity, CERT-GOV-MD was set up within the Special Telecomunication Centre. This is a governmental CERT, charged with cyber incident handling for government networks and systems. The 'Action plan for Digital Moldova 2020 implementation' established that CERT-GOV-MD will be fortified and transformed into a national CERT.

7.2 Cybercrime strategy

Certain aspects of a cybercrime strategy are covered by the National Strategy for Information Society Development - Digital Moldova 2020 and the Action Plan on its implementation: For example, the Supreme Security Council recommended in its (above mentioned decision of 2014) that:

- 'The Prosecutor General's Office, jointly with the Government and the Intelligence and Security Service, ensure the implementation of the action plan in the field of prevention and fight against cybercrime, published in the Official Paper No 228-232/1532 18 October 2013'.
- Law 20/2009 for preventing and countering cybercrime covers some aspects regarding MLA, national cooperation and international cooperation in countering cybercrime

7.2.1 International cooperation

International cooperation is possible either pursuant to applicable international agreements, or on the basis of reciprocity. Relevant pieces of legislation are the Law of 3 February 2009 on the levels of cooperation with foreign authorities and the Law of 26 January 2010 on Preventing and Combating Cybercrime. However, the Republic of Moldova would further benefit from the continuous sharing of best practices and experiences, including by participating in additional conferences, workshops and training.[85] CERT-GOV-MD initiated bilateral and multilateral cooperation with national CERTs in the area of cybersecurity

The Republic of Moldova is a Party to the Budapest Convention on Cybercrime and participated in the assessment of the mutual legal assistance provisions of this treaty in 2013 and 2014. The recommendations adopted by the Cybercrime Convention Committee also apply to the Republic of Moldova[86].

---

[83] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems
CETS No.: 189

[84] http://cert.acad.md /

[85] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_Project_EaP/Chisinau_International_Conference_Nov2014/CyberEAP%20AssessRep_v15.pdf

[86] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf

7.2.2 Public/private cooperation

Informal arrangements have been established for the cooperation between law enforcement and ISPs.

The Ministry of Interior plans to adopt a Memorandum of Understanding with ISPs. It may take inspiration from the similar arrangement adopted in Georgia. LEAs have already been discussing this issue with ISP associations in Moldova. Given the different considerations of each ISP, it appears that individual Memorandums with specific providers may be more suitable.[87]

7.2.3 Reporting mechanism

No information available.

7.3 Republic of Moldova summary

Assessment item	**Republic of Moldova**
Cybersecurity	
Cybersecurity strategy in place	Draft
Cybersecurity strategy names preventing cybercrime as a key objective	Yes
Establishment of computer emergency response team(s), CERTs	Yes
Cooperation on both national and international level;	yes
Cooperation with private sector	Yes
Multi-stakeholder governance	Yes
Support of economic growth	No information
Mandating minimal technical safeguards	Yes
Reporting mechanism	No information
Education and capacity building	Yes
Protecting fundamental rights, freedom of expression, personal data and privacy	No information
Cybercrime	
Cybercrime strategy in place	No
Public/private cooperation	supported by CoE EAP project 2011-2014 and recommended to be continued
International cooperation	supported by CoE EAP project 2011-21 and recommended to be continued
Establishment of platforms for reporting cybercrime	supported by CoE EAP project 2011201and recommended to be continued

[87] ibid.

8 Ukraine

8.1 Cybersecurity strategy

Ukraine has prepared a draft Cybersecurity Strategy[88]. Provision for cybersecurity is regulated by its national Constitution, laws on the Main Principles of Domestic and Foreign Policy and On the Main Principles of National Security, Ukraine's National Security Strategy, Ukraine's Information Security Doctrine and the Council of Europe Convention on Cybercrime ratified by the Law of Ukraine No 2824 of 7 September 2005.

Objectives of this draft Strategy include:

- Devising main policy directions on cybersecurity, in particular, the creation of a regulatory framework , harmonised with international standards;
- Creating an advanced, flexible national cybersecurity system for efficient cooperation of government agencies responsible for the enforcement of cybersecurity;
- Creating conditions for cooperation between public and private sectors, society and the State in countering cyber-threats and for international cooperation on cybersecurity;
- Creating conditions for the protection of national information infrastructure, primarily, objects of critical information infrastructure;
- Creating conditions for the development of a system that prepares cadres in cybersecurity sphere.

Priority measures in the first implementation phase (2015 - 2016) will focus on the development and improvement of the regulatory framework, particularly to ensure the functioning of the national cybersecurity system, the preparation of the Armed Forces of Ukraine for cyber warfare, basic preparation of cadres specialising in countering cyber-threats,and conditions for cooperation between public and private security sectors on combating cybercrime and greater attention to informing the public and businesses about cybersecurity.

The second phase (2017 - 2018) is planned to focus on the improvement of international rules of conduct in cyberspace and the international regulatory framework to address cybersecurity-related challenges to national and international security, the completion of the national cybersecurity system, the implementation of programs to support domestic innovative products to enhance cybersecurity and fostering development of the computer emergency response team network in Ukraine.

The third phase (2018 and beyond) will be adjusted on the basis of the assessment of its effectiveness and emerging challenges.

8.1.1 CERT

Ukraine's CERT is the CERT-UA[89].

[88] http://www.niss.gov.ua/public/File/2013_nauk_an_rozrobku/kiberstrateg.pdf. See Oleksandr V. Potii; Oleksandr V. Korneyko; Yrii I. Gorbenko, 'Cybersecurity in Ukraine: Problems and Perspectives', http://connections-qj.org/system/files/32.01_potii_korneyko_gorbenko.pdf?download=1 for a comprehensive summary

[89] www.cert.gov.ua

8.1.2 International cooperation

The draft strategy advocates international collaboration in the following areas:

- Support international initiatives in the cybersecurity sphere considering Ukraine's national interests;
- Help prevent the militarisation of cyberspace;
- Ensure Ukraine's participation in European and regional cybersecurity enforcement systems and strictly abide by Ukraine's international obligations in cybersecurity ;
- Enhance international cooperation on combating cyber-terrorism, cybercrime and cooperation on cybersecurity at the national and departmental levels;
- Contribute to international rules of government's conduct in cyberspace and improve the international legal framework to address cybersecurity-related challenges to national and international security.

8.1.3 Public/private cooperation

The strategy outlines the importance of creating conditions for cooperation between public and private sectors, society and the State in countering cyber-threats and for international cooperation on cybersecurity.

8.1.4 Multi-stakeholder governance

In order to enhance cybersecurity, the strategy foresees that the State, in partnership with the private sector, citizens and civil society, must take part in the creation and implementation of the national strategy. Furthermore, a key element for its enforcement lies in the coordination of public authorities, institutions, private sector, research institutions, professional associations and non-governmental organisations in the cybersecurity sphere.

8.1.5 Support of economic growth

The Strategy establishes as a priority the creation of economic preconditions for the development and enforcement of security of the national information infrastructure and its resources.

8.1.6 Mandating minimal technical safeguards

Cyber protection is defined as a set of organisational, regulatory, military, operational and technical measures with the aim of enforcing cybersecurity. The strategy should include a clause regarding strict compliance with legal provisions protecting government information resources, cryptographic and technical protection of information, including protection of personal information by the heads of bodies controlling objects of critical information infrastructure.

8.1.7 Education and capacity building

The Strategy refers to several areas regarding education and capacity building. For example, it recommends changes in academic plans and curricula of secondary and higher education institutions and in research and development plans of senior officials and management.

8.1.8 Protecting fundamental rights

The Strategy stresses the importance of safeguarding the rights and freedoms of Ukrainian citizens, including the right to privacy and freedom of communication. A draft law 'on the ensuring the cybersecurity of Ukraine' is in preparation[90] providing for the protection of individual and societal vital interests in cyberspace and identifying the main areas for cybersecurity enforcement.

8.2 Cybercrime strategy

There is no specific cybercrime strategy in place.

8.2.1 International Cooperation

The General Prosecutor's Office and the Ministry of Justice are jointly responsible for the handling of extradition and mutual assistance requests. A 24/7 contact centre unit has been set up within the Cybercrime Department of the Ministry of Interior.[91]

8.2.2 Public/private cooperation

The cybercrime division has been developing a Memorandum of Understanding with ISPs. The Memorandum is expected to lay out the framework for the prompt recording and retrieval of technical information about cybercrimes. However, the new Criminal Procedure Code has rendered the Memorandum illegal. The future of the Memorandum depends on whether any further amendments are made to the Criminal Procedure Code.[92]

8.2.3 Reporting mechanism

No information available.

[90] Draft Law of Ukraine 'On ensuring the cybesecurity of Urkaine', http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=47240 (accessed 12 May 2015). See Oleksandr V. Potii; Oleksandr V. Korneyko; Yrii I. Gorbenko, 'Cybersecurity in Ukraine: Problems and Perspectives', for a description of the legislative framework http://connections-qj.org/system/files/32.01_potii_korneyko_gorbenko.pdf?download=1

[91] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_Project_EaP/Chisinau_International_Conference_Nov2014/CyberEAP%20AssessRep_v15.pdf

[92] ibid.

8.3 Ukraine summary

Assessment item	Ukraine
Cybersecurity	
Cybersecurity strategy in place	Draft
Cybersecurity strategy names preventing cybercrime as a key objective	Yes, through the draft law
Establishment of computer emergency response team(s), CERTs	Yes
Cooperation on both national and international level;	Yes
Cooperation with private sector	Yes
Multi-stakeholder governance	Yes
Support of economic growth	Yes
Mandating minimal technical safeguards	Yes
Reporting mechanism	No information
Education and capacity building	Yes
Protecting fundamental rights, freedom of expression, personal data and privacy	Yes
Cybercrime	
Cybercrime strategy in place	No
Public/private cooperation	supported by CoE EAP project 2011-214 and recommended to be continued
International cooperation	supported by CoE EAP project 2011-214 and recommended to be continued
Establishment of platforms for reporting cybercrime	supported by CoE EAP project 2011-2014and recommended to be continued

9 Summary table

Cybersecurity strategy	Armenia	Azerbaijan	Belarus	Georgia	Rep. of Moldova	Ukraine
Cybersecurity strategy in place	In concept stage	Yes	No	Yes	Draft	Draft
Cybersecurity strategy names preventing cybercrime as a key objective	n/a	No	No	Yes	Yes	Yes, through the draft law
Computer emergency response team(s), CERTs	Yes	Yes	Yes	Yes	Yes	Yes
Cooperation on both national and international level;	n/a	Yes	Yes, on national level	Yes	No information	Yes
Cooperation with private sector	n/a	Yes	Yes	Yes	Yes	Yes
Multi-stakeholder governance	n/a	Yes	No information	Yes, (public sector)	Yes	Yes
Support of economic growth	n/a	Yes	Yes	Yes	No information	Yes
Mandating minimal technical safeguards	n/a	Yes	No information	Yes	Yes	Yes
Reporting mechanism	n/a	No	No information	Yes	No information	No information
Education and capacity building	n/a	Yes	Yes	Yes	Yes	Yes
Protecting fundamental rights, freedom of expression, personal data and privacy	n/a	Yes	Yes	Yes	Yes	Yes

Cybercrime strategy	Armenia	Azerbaijan	Belarus	Georgia	Rep. of Moldova	Ukraine
Cybercrime strategy in place	No information	No information	No	Yes, Organized crime strategy III Chapter	No	No
Public/private cooperation	supported by CoE EAP project 2011-2014 and recommended to be continued	No information	supported by CoE EAP project 2011-2014 and recommended to be continued	Yes, with ISP	supported by CoE EAP project 2011-2014 and recommended to be continued	supported by CoE EAP project 2011-2014 and and recommended to be continued
International cooperation	supported by CoE EAP project 2011-2014 and recommended to be continued	Yes	supported by CoE EAP project 2011-2014 and recommended to be continued	supported by CoE EAP project 2011-2014 and recommended to be continued	supported by CoE EAP project 2011-2014 and recommended to be continued	supported by CoE EAP project 2011-2014 and recommended to be continued
Establishment of platforms for reporting cybercrime	supported by CoE EAP project 2011-2014 and recommended to be continued	No information	supported by CoE EAP project 2011-2014 and recommended to be continued	supported by CoE EAP project 2011-2014 and recommended to be continued	supported by CoE EAP project 2011-2014 and recommended to be continued	supported by CoE EAP project 2011-2014 and recommended to be continued

10 Conclusions and recommendations

10.1 Conclusions

10.1.1 Status of Cybersecurity or –crime strategy

The report shows that with the exception of Belarus, all EAP countries already have or are planning to have a cybersecurity strategy and/or similar or related strategies. However, only Georgia and Azerbaijan have formal cybersecurity strategies in place, and were the two States which had adopted policy documents at the time of the meeting in Chisinau in November 2014. The other States have strategies at the draft or concept stage.

At the Kiev meeting (October 2013) participating EAP States[93] affirmed their willingness 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. Georgia, the Republic of Moldova and Ukraine affirmed that actions against cybercrime are priorities of the cybersecurity strategy. However, none of the countries reported a specific cybercrime strategy in place. Georgia was the only country to provide information on cybercrime within its Organized Crime Strategy.

On the basis of information received and publicly available, it appears that Georgia has the most mature policy on cybersecurity and -crime in place within the EAP region, and could serve as a role model for the other countries.

10.1.2 Collaboration and regional approach

Several EAP members stressed the need to bring together all national expertise available in order to effectively tackle the many dimensions and cross-border nature of cybersecurity and cybercrime. Hence, strengthening national and international collaboration and public private partnership are mentioned in the strategies of Azerbaijan, Belarus, Georgia, Moldova and Ukraine.

While some countries within the EAP region cooperate on a national level (e.g. Azerbaijan and Ukraine), there seems to be no overarching regional approach on cybersecurity topics outside the remit of the Council of Europe's EAP activities.

10.2 Recommendations

10.2.1 Refine approaches to cybersecurity

It is recommended that the Armenia, Belarus, Republic of Moldova and Ukraine further develop their strategies considering the criteria set out in this report. The Cybersecurity strategy of Georgia may serve as an example for the EAP region. Furthermore, EAP countries should consider organised crime strategies to include cyber offences committed by means of computer system, also referring to the Georgian model.

The following are some basic recommendations, which can help build a resilient and sustainable cybersecurity policy:

- The state should assume the coordination role for public institutions and private corporations;
- The stakeholders involved at national level in cyberstrategy elaboration should define and accept the basic terms (cybersecurity and cybercrime);
- A coordination committee should be convened prior to elaboration of a cyberstrategy, to coordinate all stakeholders, monitor their compliance with their statutory remit and

[93] Armenia, Belarus, Georgia, Republic of Moldova and Ukraine.

responsibilities (in particular public institutions), and provide correct information for the first stage of the strategy elaboration;
- Public institution experts should play a primary role the first stage of elaboration, representing institutions in working groups or committees, conducting the evaluation of their respective structures, and taking a global view regarding cyber security issues;
- Cybersecurity is not cybercrime and as a consequence cybersecurity strategy is not covering all aspects needed for a cybercrime strategy;
- Cybersecurity strategy must address the specific national context;
- Public and private resources must be jointly applied;
- The private sector should be involved in elaborating cybersecurity strategies from the twin perspective of cybersecurity consumers and cybersecurity providers; they should respectively focus on major threats and not try to address all issues;
- International cooperation is important but inter-agency cooperation on a national level is mandatory;
- Cyberstrategy operations should be developed gradually among entities and/or people who have a trusted relationship;
- Cyberstratgies should be open to insights from third parties with different knowledge and expertise;
- Cyberstrategies should define how information is to be collected, by which entity and how it is to be shared among agencies and authorities;
- It is of utmost importance that cybersecurity or cybercrime strategies have clear performance indicators both qualitative and quantitive to assess when Strategic Priorities are met (the Georgian Cybersecurity/Cybercrime Strategic goals performance monitoring system may serve as a good practice for other EAP Countries)

10.2.2 Stronger emphasis on the criminal justice approach to cybercrime and electronic evidence

Regarding cybercrime, whether or not a dedicated cybecrime strategy has been elaborated, the general policies on crime or strategies on organised crime should address the principal aspects of cybercrime and electronic evidence:

- Legal framework providing in particular specific procedural law powers to secure electronic evidence which are to be subject to rule of law and human rights conditions and safeguards;
- Institutional developments (investigative, forensic and Internet investigative capacities – Cyber patrols);
- Appropiate equipment and training for LEA;
- Private-sector cooperation and partnerships, not only for investigative purposes, but for reporting and education purposes;
- Inclusion of concrete cybercrime-related activities in the action/work plans of the police (Specialised Departments for investigation, digital forensic, training, etc);
- More effective international cooperation on cybercrime and electronic evidence[94].

10.2.3 Build incident response capabilities

All EAP countries have CERTs in place. All EAP countries are a member of IMPACT, the ITU (International Telecommunication Union) initiative on cybersecurity assistance[95]. With the exception of Armenia and the Republic of Moldova, all EAP CERTs are members of the FIRST (Forum of Incident Response and Security Teams) organisation. FIRST arranges conferences and

[94] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf

[95] http://www.impact-alliance.org/countries/alphabetical-list.html

takes part in development activities for CERTs and brings together product security teams from government, commercial, and the academic sector.

However, not all EAP CERTs appear to have the same level of maturity; e.g. the Georgian CERT publishes recent information about its activity on its website, while, for example, both the Armenian and Moldovan CERT web pages present outdated information[96]. While this report cannot give a conclusive statement about the CERT effectiveness, it is suggested that EAP countries make it a priority to strengthen and develop their CERT's capabilities. Furthermore, it is suggested that all EAP countries link with their counterparts from private sector within their country and their international counterparts to enhance situational awareness and response capabilities.

The place and role of CERT should be very well defined, in order not to create confusion or overlap with other institutions. CERT should be responsible for cybersecurity policy and play an important role in the coordination mechanism for incident response. Instruments given to CERT are very important in order to fulfil their tasks. For example, it is important for CERT to have a data base with cyber incidents, analytical capacities for investigating incidents and a direct connection and cooperation with LEA in order to report illegal activities, reduce risks and decide the security measure to be implemented.

With the exception of Georgia, no reporting mechanism seems to be in place. It is suggested to link the reporting activities with the cybercrime reporting activities according to the 'Good practice study on cybercrime reporting mechanisms', prepared under the GLACY project.

The existence of an operational national CERT could be helpful for countering cybercrime too. Even though CERTs are not LEAs, at present the biggest quantity of data related to cyber incidents is retained and circulated by professional bodies such as the CERTs or CSIRTs. The experts of these structures could categorise these incidents in a kind of triage, sorting and transferring them to the institutions with the relevant remit. For example, a national CERT in receipt of information (in the scope of its responsibilities as a national PoC) from ISPs regarding suspected malicious activities, after analysis of indicators of compromise with potential for different types of crimes, could transfer that information to the relevant police cyber unit, to the governmental CERT or to national intelligence.

10.2.4 Develop an Action plan for implementation of the cybersecurity strategy

The action plan should include activities for the authorities responsible with prevention and fighting against cybercrime including cybersecurity in order to implement the main concepts from the cybersecurity strategy (define critical infrastructure, create the early warning system, coordination body/entity for cyber incident/attacks, response procedures).

10.2.5 Develop international cooperation

Azerbaijan, Belarus, Georgia and Ukraine identify international cooperation as a prioritiy. Some regional knowhow exchange is already established but it is suggested that countries engage in international cooperation to the widest extent possible. This may require them to extend regional approaches to cybersecurity, participate in international cyber exercises (e.g. ENISA Cyber Europe exercise tentatively to be held in 2016[97]) or attend events that help to build capacity (e.g annual FIRST conference, Global Conference on Cyberspace 2015 in the Hague, Netherlands). This not only applies to technical expertise but also to the policy area.

[96] The governmental Moldovan CERT which is to become the national CERT has updated information http://cert.gov.md/about-us/about-cert-gov-md.html.

[97] http://www.enisa.europa.eu/media/press-releases/biggest-eu-cyber-security-exercise-to-date-cyber-europe-2014-taking-place-today

Due to the crossborder characteristics of cybercrime, the solution of cyber crime cases requires the support of other states. But, international cooperation can be structured on different levels: The cybersecurity strategy should specify the competence of particular authorities in the domains of NIS, cybercrime or cyberdefence. National authorities cooperate more efficiently with their direct foreign counterparts: one state's CERT with another state's CERT, a national police unit with another national police unit.

With the exception of Belarus, the other EAP countries are Parties to the Budapest Convention on Cybercrime and participated in the assessment of the mutual legal assistance provisions of this treaty in 2013 and 2014. The recommendations adopted by the Cybercrime Convention Committee also apply to all EAP countries[98]. Full implementation will certainly lead to a major improvement in international cooperation on cybercrime and electronic evidence.

10.2.6 Adopt a multi-stakeholder approach

A multi-stakeholder approach is included as an element of all the cybersecurity strategies available, with the exceptions of the Armenia and Belarus. For the implementation of this approach, all national stakeholders from the public and private sector should be involved in the development, implementation and enforcement of a cybersecurity strategy. A National Cybersecurity Council, consisting of public sector entities (such as National Security, Ministry of Interior, and Telecommunications Agency), private sector entities (banks, ISPs, telecommunication providers, international software and hardware companies) and academics could coordinate cybersecurity, while respecting and observing one another's interests. Such an approach should be supported by a legal framework setting out rights and obligations of all stakeholders, procedures for information exchange and modes of cooperation.

A suggested model is the Dutch National Cybersecurity Council[99] set up to define the cyber-approach and related national prioririte s. Another model is the Romanian Operational Council for Cybersecurity, headed by the Presidential Counselor for National Security as Chairman and the Prime Minister's Counselor for National Security as Deputy. This council includes representatives at state secretary level of each institution with responsibilities in cybersecurity, who are also involved in the elaboration of the cybersecurity strategy. The Estonian Cyber Security Council offers another useful model.

10.2.7 Moderate the role of national security in cyberstrategies

As the nature of cybercrime has changed, certain cybercrime offences have or may come to be regarded as threats to national security. In addition to the conventional criminal police, security services may have a role. If security authorites have been vested with investigative powers and the right to initiate and conduct criminal investigations, a clear and precise legal framework must be elaborated. Otherwise, citizens and the private sector will face uncertainty regarding matters such as authority, procedures, and basis for issuing a Law Enforcement Request or National Security Order (which government entity has authority to issue them, how they are handled and governed, and for what purposes). Such uncertainty may hamper collaboration between government agencies and with the private sector, as well as international cooperation. Azerbaijan, Georgia, the Republic of Moldova and Ukraine have all stressed a multi-governance approach, which can mitigate the risk of National Security considerations taking precedence over human rights requirements.

Cybersecurity is a complex concept, which, in some countries also includes cybercrime. There remains a need for delineating responsibilities among authorities. Cybercrime should be a

[98] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf

[99] http://www.infosecisland.com/blogview/14968-Dutch-Cyber-Security-Council-Now-Operational.html

responsibility for the LEA and clear distinctions related to cybersecurity should be included in the strategies, policies or other national plans. Different strategies for cybercrime and cybersecurity could be an option but a mechanism for coordination and cooperation between different authorities should be implemented.

While increased collaboration between government entities at national and international level is absolutely vital for the success of a holistic 'cyber' approach in executing a cyberstrategy, careful consideration should be given to how national laws and policies are formulated. Furthermore, joint strategies tend to focus on the area of offences against the confidentiality, integrity and availability of computer data and systems, omitting offences committed by means of computer systems and thereby neglecting one of the main aspects of cybercrime. Again, the Organized Crime Strategy of Georgia may serve as a model for other EAP countries.

10.2.8 Incentivise adherence to minimal technical safeguards

With the exception of Armenia and Belarus, all other EAP countries assert mandating technical standards as a priority. However, the strategies fail to specify the relevant standards. As a minimum, strategies should serve as a basis for the issuance of regulations obliging Critical Informational System subjects to prescribe to minimal cybersecurity standards for the IT technologies in their jurisdiction. Sectoral standards are already available for certain areas (e.g finance sector).

Although self-regulation can be effective, governments should bear in mind that it might not suffice for Critical Infrastructure. In the face of public expectations of enhanced security but limited private willingness to invest in security, governments should seek to establish mandatory standards and supervision.

It is suggested that the private sector be incentivised (e.g. through voluntary certification) to meet technical safeguards in order to achieve a swift adoption of standards, and thus avoid penalisation in the event of an incident. By adopting this positive approach, public-private cooperation and information sharing can be enhanced.

10.2.9 Invest in research, technology and capacity building

A number of countries were concerned about the lack of talented cyber-security people in the public sector, as they compete with the private sector that often offers better benefits and compensation programmes. By adopting a multi-stakeholder approach, these private sector cybersecurity and cybercrime experts (e.g. within banking, computer industry, ISPs) can still be part of the overall national cybersecurity programme and support national capacity building and the respective cyber-network. A good example of a joint private and public sector initiative is the Estonian Cyber Defence League.[100] In addition, an academic research agenda derived from the cyber-strategy should be built to support government activities in this area.

---

[100] http://www.kaitseliit.ee/en/cyber-unit