Bucharest, January 2019

Cybercrime and cybersecurity strategies in the Eastern Partnership region

Updated report 2018

Results of series of national workshops
Eastern Partnership countries
PGG 2018: Cybercrime@EaP project
February - May 2018

This project is funded by the European Union and the Council of Europe and implemented by the Council of Europe

Partnership for Good Governance

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Contact

Giorgi.Jokhadze@coe.int
Cybercrime Programme Office of the Council of Europe (C-PROC)
Bucharest, Romania

Disclaimer

This document has been produced as part of a project co-funded by the European Union and the Council of Europe, with inputs from experts Daniel Ionita (Romania), Nigel Jones (United Kingdom) and Markko Kunnapu (Estonia). The views expressed herein can in no way be taken to reflect the official opinion of either party.

Contents

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	Mutual Legal 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

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.

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[1]:

- 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.

The PGG 2018: Cybercrime@EAP project, implemented by the Cybercrime Programme Office of the Council of Europe, aims to support this process in the Eastern Partnership by conducting region-wide studies on cybercrime threats and state of cybercrime strategies. Conducted as series of workshops throughout the Eastern Partnership countries from February to May 2018, all relevant stakeholders – criminal justice agencies, policy makers, cyber security experts and the Internet industry – were engaged in discussions moderated by international experts, with a view to map and analyze their tasks and responsibilities for security of cyberspace, perception of threats of cybercrime and cybersecurity, and possible strategic responses to these threats.

1 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680300ad4

The current study is thus an attempt to update the existing Study on Cybercrime and cybersecurity strategies in the Eastern Partnership region (2015) with data obtained through discussions with national stakeholders regarding threats and challenges of cybercrime during the above-noted workshops.

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.

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[2]), 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.

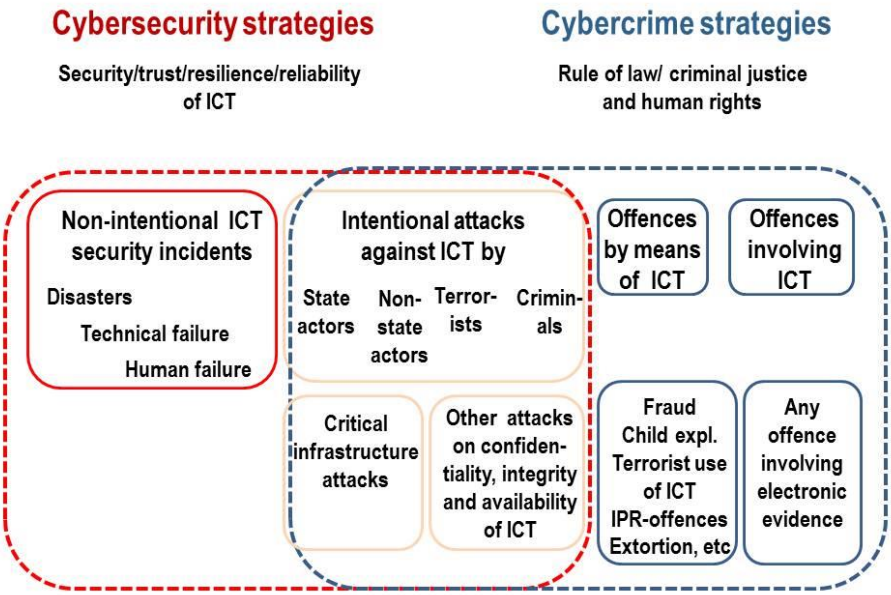
The questions of cybersecurity and cybercrime are thus closely connected with regard to intentional attacks against computer data and systems. Cybersecurity and cybercrime are mutually reinforcing even though they follow a different rationale:

- 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.

[2] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e1 (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. 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.

As many other states around the worlds, states of the Eastern Partnership region have been the target of serious cyber-attacks and other security incidents in recent years. They thus recognise the growing challenges and threats in cyberspace and the need to respond, among other things, through the means of criminal justice. All countries in the EAP region face similar threats in cyberspace as other counties, which can be grouped into three 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.
- 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.
- 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.

At the same time, individual threat landscapes in each of the Eastern Partnership countries differ from each other rather significantly. While some of this can be attributed to perception-based nature of the exercise that led to production of this report, and with the majority of stakeholders involved still being the state agencies tasked with cybercrime and cybersecurity, it is nevertheless apparent that the states of the region view their priorities for security of cyberspace, including through criminal justice response, rather differently. On the level of individual threats, perhaps only malware (including ransomware) and phishing could be deemed as strong showing consistently across the Eastern Partnership; these, however, represent a reflection of global trends of cybercrime overall[3] rather than a specific uniform feature of the Eastern Partnership, and thus should not be taken as such.

Similar to the previous report, the EAP region retains its potential a platform to carry out cybercrime activities with targets elsewhere; the recent examples of ransomware attacks such as WannaCry, NotPetya and Black Energy further support this view. According to the 2018 Internet Organised Crime Threat Assessment ('iOCTA') prepared by Europol's European Cybercrime Centre (EC3), some EaP states are either targets or origins of attacks suspected to be state-sponsored, condoned or otherwise not financially motivated, as well as cyber-attacks causing some disruption to critical infrastructure industries in the EU from beyond.[4]

When it comes to challenges, however, the need for public-private cooperation and stronger awareness are rather consistent across the states of the region. 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.

[3] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment

[4] See iOCTA report (2018), especially pp. 21 and 28.

1.4 Outline of the report

Section 2 describes the current status and comparative developments regarding cybersecurity and cybercrime strategies outside the EAP region, such as the EU policies, ENISA, Estonia and the UK experience.

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

Cybersecurity is critical to both prosperity and security. As our daily lives and economies increasingly rely on digital technologies, we become more and more exposed to malicious cyber-attacks. These are spreading in terms of both who is involved and what they seek to achieve. Harmful and hostile cyber activities have both criminal and political motivations, threatening our economies, democratic freedoms and values; thus the vulnerability of evolving economic and public infrastructure has been put into focus.

2.1 Developments in the cybersecurity policy area

2.1.1 European Union Cybersecurity Environment

The EU's objective is to ensure more resilient digital systems in every walk of life. This is a collective challenge needing a comprehensive approach. It needs the right structures to push higher standards in terms of how we protect ourselves against attacks through a stronger shield, how we detect attacks, and how we respond. This requires a major upscaling of the EU's technological capabilities to provide strategic autonomy in cyberspace. It also requires a paradigm shift to treat cybersecurity as a common societal challenge and to engage every layer of government and society in efforts to make Europe more secure.

On 13 September 2017, in the context of its Digital Single Market Strategy, the Commission adopted and transmitted to the Council and to the European Parliament the REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity European Union Agency for Cybersecurity", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'') with Article 114 TFEU as a legal basis. As a part of the so-called 'Cybersecurity package', this proposal aims at a high level of cybersecurity, cyber resilience and trust within the Union with a view to ensuring the proper functioning of the internal market.

In October 2017, the European Council called for the Commission's cybersecurity proposals to be developed in a holistic way, delivered timely and examined without delay, on the basis of an action plan to be set up by the Council. On 12 December 2017, the General Affairs Council adopted the Action Plan for the implementation of the Council Conclusions on the Joint Communication to the European Parliament and the Council: 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU'. The Action Plan reflected the Council's ambition to achieve a general approach on the proposal by June 2018. There were 12 meetings held in Horizontal Working Parties on Cyber Issues on this proposal which resulted in eight consecutive revised versions of the proposal with a view to agreeing on a general approach at the TTE (Telecom) Council and that happened on 8 June 2018. Currently, the proposal is in a process of trialogue and is shaping up as legislative act of the European Parliament, to be adopted most probably in its last legislative session in March 2019.

In 2016, the Union adopted the first legislative act in the area of cybersecurity, the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive").

The NIS Directive is the first piece of EU legislation specifically aimed at improving cybersecurity throughout the Union. By ratifying a definite number of obligations across the EU, the Directive will help ensure a consistent approach to cybersecurity "with a view to achieving a high common level of security of networks and information systems within the Union so as to improve the functioning of the internal market". The main points of the NIS Directive can be summarised as follows:

- improved cybersecurity capabilities at national level,
- increased EU-level cooperation,
- security measures and incident reporting obligations for Operators of Essential Services (OES) and Digital Service Providers (DSP).

According to one of the provisions of the NISD, Member States must ensure that DSPs notify the competent authority without undue delay of any incident having a substantial impact on the provision of a service. In determining the "substantial impact", the Directive mentions just five indicators to be used without providing other details.

As the Directive provides only a sketchy description of the incident notification concepts and the overall process, the main goal of this document is to develop a set of guidelines for all concerned stakeholders (EU level authorities, public, private), aimed at supporting the implementation of the NIS Directive requirements regarding mandatory incident notification for Digital Service Providers.

2.1.2 European Network Information Security Agency (ENISA)

In 2004, the European Parliament and the Council adopted Regulation (EC) No 460/20048 establishing ENISA with the purpose of contributing to the goals of ensuring a high level of network and information security within the Union, and developing a culture of network and information security for the benefit of citizens, consumers, enterprises and public administrations. In 2008, the European Parliament and the Council adopted Regulation (EC) No 1007/20089 extending the mandate of the Agency until March 2012. Regulation (EC) No 580/201110 extended further the mandate of the Agency until 13 September 2013. In 2013, the European Parliament and the Council adopted Regulation (EU) No 526/201311 concerning ENISA and repealing Regulation (EC) No 460/2004, which extended the Agency's mandate until June 2020.

Based on the mandate entrusted to it, ENISA supports the European Institutions, the Member States and the business community in addressing, responding and especially preventing network and information security problems. It does so through a series of activities across five areas identified in its strategy, adopted by the Management Board in 2016:

- **Expertise**: provision of information and expertise on key network and information security issues.
- **Policy**: support to policy making and implementation in the Union.
- **Capacity**: support to capacity building across the Union (e.g. through trainings, recommendations, awareness raising).
- **Community**: foster the network and information security community [e.g. support to the Computer Emergency Response Teams (CERTs), coordination of cyber exercises].
- **Enabling** (e.g. engagement with the stakeholders and international relations).

The September 2017 proposal of Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity European Union Agency for Cybersecurity", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act''), which has reached on general approach on June 2018, lays down the objectives, tasks and organisational aspects of ENISA – the EU Cybersecurity Agency and creates a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity of ICT products and services in the Union.

The proposed Regulation contains two major strands:

- a permanent mandate for the Agency with a delineated scope in view of the needs under the new policy priorities and instruments, and a renewed set of tasks and functions for

the Agency, to allow effective and efficient support to Member States, EU institutions and other stakeholders' efforts in view of ensuring a secure cyberspace;

- a European cybersecurity certification framework for ICT products and services and rules governing European cybersecurity certification schemes allowing certificates issued under those schemes to be valid and recognised across all Member States and addressing the current market fragmentation.

A key role was attributed to ENISA in supporting implementation of the NIS Directive. In addition, effective fight against cybercrime is an important priority in the European Agenda on Security, contributing to the overall aim of achieving a high level of cybersecurity.

The Agency established by this Regulation should succeed ENISA as established by Regulation (EU) No 526/2013. The Agency should carry out the tasks conferred on it by the Regulation and legal acts of the Union in the field of cybersecurity by, among other things, providing expertise and advice and acting as a Union centre of information and knowledge. It should promote the exchange of best practices between Member States and private stakeholders, offering policy suggestions to the European Commission and Member States, acting as a reference point for Union sectoral policy initiatives with regard to cybersecurity matters, fostering operational cooperation between the Member States and between the Member States and the European institutions, agencies and bodies.

2.1.3 European Cybersecurity Industrial, Technology and Research Competence with a network of National Coordination Centres

The creation in 2016 of the Public-Private Partnership ('cPPP') on cybersecurity in the Union was a solid first step bringing together the research, industry and public sector communities to facilitate research and innovation in cybersecurity and within the limits of the 2014-2020 financial framework should result in good, more focused outcomes in research and innovation. The cPPP allowed industrial partners to express commitment about their individual spending on areas defined in the partnership's Strategic Research and Innovation Agenda.

The Heads of State and Government at the Tallinn Digital Summit, in September 2017, called for the Union to become "a global leader in cyber-security by 2025, in order to ensure trust, confidence and protection of our citizens, consumers and enterprises online and to enable a free and law-governed internet."

The Digital Europe Programme proposed by the Commission in June 2018 seeks to enlarge and maximise the benefits of digital transformation for European citizens and businesses in all relevant EU policy areas, reinforcing the policies and supporting the ambitions of the Digital Single Market. The programme proposes a coherent and overarching approach to ensuring the best use of advanced technologies and the right combination of technical capacity and human competence for the digital transformation – not only in the area of cybersecurity, but also as regards to smart data infrastructure, artificial intelligence, advanced skills and applications in industry and in areas of public interest. These elements are interdependent, mutually reinforcing and, when fostered simultaneously, can achieve the scale necessary to allow a data economy to thrive. The Horizon Europe Programme - the next EU R&I Framework programme also puts cybersecurity among its priorities.

In this context Commission elaborated a proposal to set-up of a **European Cybersecurity Industrial, Technology and Research Competence** with a network of **National Coordination Centres**. This made-for-purpose cooperation model should work as follows in order to stimulate the European cybersecurity technological and industrial ecosystem: the Competence Centre will **facilitate and help coordinate the work** of the Network and nurture the Cybersecurity

Competence Community, driving the cybersecurity technological agenda and facilitating access to the expertise so gathered.

In addition, the European Cybersecurity Industrial, Technology and Research Competence Centre should also seek **to enhance synergies between the civilian and defence dimensions of cybersecurity**. It should give support to Member States and other relevant actors by providing advice, sharing expertise and facilitating collaboration with regard to project and actions. When requested by Member States it could also act as a project manager notably in relation to the European Defence Fund. The present initiative aims to contribute to tackling the following problems:

- **Insufficient cooperation between cybersecurity demand and supply industries**. The European businesses face the challenge of both remaining secure and offering secure products and services to their clients. Yet, often they are not able to appropriately secure their existing products, services and assets or to design secure innovative products and services. Key cybersecurity assets are often too costly to be developed and set up by individual players, whose core business activity is not related to cybersecurity. At the same time, the links between the demand and supply side of the cybersecurity market are not sufficiently well developed resulting in sub-optimal supply of European products and solutions adapted to different sectors' needs, as well as in insufficient levels of trust among market players.
- **Lack of an efficient cooperation mechanism among Member States for industrial capacity building**. At the moment, there is also no efficient cooperation mechanism for Member States to work together towards building necessary capabilities supporting cybersecurity innovation across industrial sectors and deployment of cutting-edge European cybersecurity solutions. The existing cooperation mechanisms for Member States in the field of cybersecurity under Directive (EU) 2016/1148 do not envisage this type of activities in their mandate.
- **Insufficient cooperation within and between research and industrial communities**. Despite Europe's theoretical capacity to cover the full cybersecurity value chain, there are relevant cybersecurity sectors (e.g. energy, space, defence, transport) and sub-domains that are today poorly supported by the research community, or supported only by a limited number of centres (e.g. post-quantum and quantum cryptography, trust and cybersecurity in AI). While this collaboration obviously exists, it is very often a short-term, consultancy-type of arrangement, which does not allow engaging in long-term research plans to solve cybersecurity industrial challenges.
- **Insufficient cooperation between civilian and defence cybersecurity research and innovation communities**. The problem of insufficient levels of cooperation also concerns the civilian and defence communities. The existing synergies are not used to the full extent due to lack of efficient mechanisms allowing these communities to cooperate efficiently and build trust, which, even more than in other fields, is a prerequisite for successful cooperation. This is coupled with limited financial capabilities in the EU cybersecurity market, including insufficient funds to support innovation.
- **Consistency with existing policy provisions in the policy area**. The Cybersecurity competence network and the European Cybersecurity Industrial, Technology and Research Competence Centre will act as an additional support to existing cybersecurity policy provisions and actors. The mandate of the European Cybersecurity Industrial, Technology and Research Competence Centre will be complementary to ENISA’s efforts but has a different focus and requires a different set of skills. While ENISA's mandate envisages an advising role on cybersecurity research and innovation in the EU, its proposed mandate focuses first and foremost on other tasks crucial for strengthening cybersecurity resilience in the EU.
- **Consistency with other Union policies**. The European Cybersecurity Industrial, Technology and Research Competence Centre will act as a single implementation body

for various Union programmes supporting cybersecurity (Digital Europe Programme and Horizon Europe) and enhance coherence and synergies between them. This initiative will also allow to complement the efforts of the Member States by providing appropriate input to education policy makers in order to enhance cybersecurity skills (e.g. by developing cybersecurity curricula in civilian and military educational systems) to help develop a qualified EU cybersecurity workforce – a key asset for cybersecurity companies as well as other industries with a stake in cybersecurity.

Such a comprehensive approach would allow supporting cybersecurity across the entire value chain, from research to supporting the deployment and uptake of key technologies. The proposal is under discussion and stipulates that the Centre will be established from January 2021 to December 2029.

2.1.4 Cybersecurity strategy of the United Kingdom

The cybersecurity strategy[5], 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[6]', the cybersecurity information sharing partnership (CISP)[7] and the cyber essentials scheme[8], which promotes voluntary cyber certifications for businesses. The UK also launched its first national computer emergency response team, CERT-UK[9] 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.

The latest national cybersecurity strategy[10], covering the period 2016 to 2021, sets out the plan to make Britain confident, capable and resilient in a fast-moving digital world. The strategy focuses on raising the cost of mounting an attack against anyone in the UK, both through stronger defences and better cyber skills. This is no longer just an issue for the IT department but for the whole workforce. Cyber skills need to reach into every profession. The government is investing £1.9 billion over the lifetime of the strategy to transform the UK's cybersecurity. This includes the creation of two cyber innovation centres to drive development of cutting-edge cyber products and dynamic new cyber security companies.

The objectives of the strategy are set out as follows:

[5] https://www.gov.uk/government/publications/cyber-security-strategy

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

[7] https://www.cert.gov.uk/cisp/

[8] https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

[9] http://www.cesg.gov.uk/Pages/homepage.aspx

[10] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

- **DEFEND**: Have the means to defend the UK against evolving cyber threats, to respond effectively to incidents, to ensure UK networks, data and systems are protected and resilient. Citizens, businesses and the public sector have the knowledge and ability to defend themselves.
- **DETER**: The UK will be a hard target for all forms of aggression in cyberspace. We detect, understand, investigate and disrupt hostile action taken against us, pursuing and prosecuting offenders. We have the means to take offensive action in cyberspace, should we choose to do so.
- **DEVELOP**: Have an innovative, growing cyber security industry, underpinned by world leading scientific research and development. We have a self-sustaining pipeline of talent providing the skills to meet our national needs across the public and private sectors. Our cutting-edge analysis and expertise will enable the UK to meet and overcome future threats and challenges.

The strategy highlights the nature of the threats faced by the UK. These include:

- Cybercriminals in the context of the interrelated forms of criminality: a. Cyber dependent crime and b. Cyber enabled crime;
- States and state sponsored threats – regular attempts are seen where states and state sponsored groups, seek to penetrate UK networks for political, diplomatic, technological, commercial and strategic advantage;
- Terrorists - Terrorist groups continue to aspire to conduct damaging cyber activity against the UK and its interests;
- Hacktivists - Hacktivist groups are decentralised and issue-orientated. They form and select their targets in response to perceived grievances, introducing a vigilante quality to many of their acts;
- Script kiddies - So-called 'script kiddies' – generally less skilled individuals who use scripts or programmes developed by others to conduct cyber attacks – are not assessed as posing a substantive threat to the wider economy or society.

The UK has created a National Cyber Security Centre (NCSC) to be the authority on the UK's cyber security environment, sharing knowledge, addressing systemic vulnerabilities and providing leadership on key national cyber security issues. The National Cyber Security Centre (NCSC) is the UK's authority on cyber security. They are a part of GCHQ. The NCSC brings together and replaces CESG (the information security arm of GCHQ), the Centre for Cyber Assessment (CCA), Computer Emergency Response Team UK (CERT UK) and the cyber-related responsibilities of the Centre for the Protection of National Infrastructure (CPNI).

The UK included in the 2106 strategy, a number of initiatives brought forward from the previous strategy. These include:

- The 'ten steps to cybersecurity[11]
- The cybersecurity information sharing partnership (CISP)[12]
- The cyber essentials scheme[13], which promotes voluntary cyber certifications for businesses.

The UK also incorporated the national CERT within the NCSC. This continues to liaise with UK businesses and other CERTs – including those in financial services and education – on cybersecurity issues, and in particular those relating to national infrastructure.

[11] https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

[12] https://www.ncsc.gov.uk/cisp

[13] https://www.ncsc.gov.uk/scheme/cyber-essentials

All cybercrime reports are now made to a single reporting point, Action Fraud (AF)[14], which also hosts the National Fraud Intelligence Bureau (NFIB). Within the National Crime Agency (NCA), sits the National Cybercrime Unit (NCCU), which leads the UK's response to cyber crime, supports partners with specialist capabilities and coordinates the national response to the most serious of cyber crime threats.

2.1.5 Cybersecurity strategy of Estonia

Estonia has paid a lot of attention to cybersecurity since 2007 and now is in the process of drafting its third governmental strategy on cybersecurity. Since the beginning Estonia has been of the opinion that in order to ensure safety and security in cyberspace a holistic approach must be followed, all stakeholders involved and joint responsibility pursued for both public and private sectors.

Since 2008 the main goals have been the same, however in later strategies government has tried to set not only higher goals, but also new and more detailed ones.

The first Cyber Security Strategy 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[15] in May 2008.

The strategy referred to the asymmetrical threats in cyberspace and considered the cyber attacks 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 operation of information systems;
- 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.

[14] https://www.actionfraud.police.uk/

[15] http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf

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[16] 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 sub-goals:

- 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.

In 2017 preparations started for the third governmental Cybersecurity Strategy. The third strategy is planned for the period 2019-2020, is based on the earlier strategies, experiences and lessons learned and sets new goals and activities. As of November 2018, the draft text has been prepared and been consulted with relevant ministries and other stakeholders. The adoption is expected by the end of 2018.

The main ideas and principles are the same as in earlier documents. Still some new ideas and aims have been introduced. Protection of fundamental rights both online and offline is important and the task of the government is to ensure safety and seamless operation of cyberspace. Safety and security is based on joint actions and competences of government authorities as well as private sector and academia. Cybersecurity should also be considered as a catalyst or enables of digital economy. In order to ensure security and safety in cyberspace technical measures need to be used including strong cryptographic solutions. One of the main principles is also transparency and communication. If incidents occur, the related information should be made public as much as possible.

Information security has been and is also one of the main pillars of the third strategy. New services and information systems need to be based on security and privacy by design. Special

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

attention has to be paid on interconnected information systems and services. Interdependency on both national and international level is crucial.

Government should have an overview of the situation in cyberspace, including threats and incidents. Awareness raising and education are the key factors and therefore information security trainings and campaigns need to be included in educational curricula.

Although organizational framework had been reviewed and capability of different governmental authorities raised, it still cannot be considered sufficient. Therefore the third strategy proposes to establish National Cybersecurity Centre.

Prevention and response to cyber threats is a joint responsibility and therefore all government stakeholders need to increase their capacity. Fight against cybercrime is a priority and more focus on national and international cooperation is needed. In order to improve cooperation at national level additional cooperation agreements need to be in place to facilitate information exchange.

Compared to the previous versions new strategy focuses more on digital economy and cybersecurity as the source of potential growth to economy. Government needs to support research and development as well as competitive and sustainable cybersecurity industry.

As cybersecurity is horizontal issue, there has to be coherence also with other policies and strategies. Cybersecurity, being part of national security, has to be also priority for the intelligence and military. Due to the technological developments, new trends and threats have emerged, including against democracy and elections and therefore competent authorities need to be able to detect and respond to those threats.

2.1.6 Good practice study on cybercrime reporting mechanisms

In September 2014, the Council of Europe published a *Good practice study on cybercrime reporting mechanisms*[17]. 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.

17 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168030287c

2.2 Selection of assessment criteria based on current developments

2.2.1 Assessment criteria for a cybersecurity strategy

Analyzing the above examples, 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;
- 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).

As there is varying degree of information collected from individual EaP countries, information on the specific points listed above will be included in the country summary. The main focus of the report will be maintained on policies, institutions and public/private cooperation as having the most relevance to cybercrime policies as well.

2.2.2 Assessment criteria for a cybercrime strategy

The approach of many countries and institutions listed in the section 'International Developments': is to address the issue of cybersecurity and cybercrime 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:[18]

- 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[19].

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

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

For the purposes of the present report, the assessment will primarily focus on elements of policies, institutional setup, international cooperation, public/private cooperation and cybercrime reporting systems. However, where information about other elements as recommended by the 2013 Declaration on Strategic Priorities for the Cooperation against Cybercrime in the Eastern Partnership Region is available, it will be also reflected in the report.

2.2.3 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.

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
Cybercrime	
Cybercrime strategy in place	Yes/no/remarks
Specialized cybercrime units	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

3.1.1 Policy framework

Although Armenia has not published a formal cybersecurity strategy, the National Security Service (NSS) is responsible for cybersecurity policy and the protection of government websites and networks. Furthermore, a concept for an Information Security Strategy was developed in 2009, which outlines certain activities to be implemented. The Digital Society 2020 Strategy includes certain measures regarding cybersecurity activities and laws in the area of cybersecurity and data protection, and is currently under discussion. Annex 4 to the draft "Concept of E-Society development in Armenia" (2010) provides for the establishment of cyber-security working group, headed by the National Security Service, was tasked with the development of an action plan with the following elements: risk assessment, cyber security legislation, capacity building, compliance with ITU and ISO standards, sector-specific approaches, development of cybercrime legislation, awareness raising, training and establishment of coordination centre. No further progress has been noted regarding this draft.

Regarding to protecting critical infrastructure against cyber threats, the Ministry of Transport, Communications and Information Technology elaborated some policies in the reference domain and implementing of this are in responsibilities of each sector competent authority (railway, airway, roadway, etc.). The critical infrastructure and any other vital services are subject of the National Security Services protection. They are also in charge also with sensitive information.

In September of 2017, the Concept Paper of Information Security Strategy was approved by the Ministry of Transport, Communications and Information Technology, the document considered to be the basis for elaborating a new strategy. In this document, there are provisions regarding information security, cybercrime and data protection. Cyber security is considered part of information security.

A working group in charge with drafting the strategy was set up. The progress can be considered at an initial level.

3.1.2 Institutional framework

CERT.AM is the non-governmental academic CERT (Computer Emergency Response Team) operating in Armenia. It is administered by a representative of the Armenian Internet domain. The establishment of the CERT-AM was mandated via Internet Society of Armenia decision on 1/09/2007.

AM NREN CSIRT is Armenia National Research and Education Network Computer Security Incident Response Team. It is administered by the representative of a major Armenian NREN which is ASNET-AM. CERT AM/AM NREN CSIRT is a national information security centre operating under the management of the Internet Society of Armenia[20].

CERT.AM / AM NREN CSIRT collects and analyzes computer incident cases (i.e. attempts or facts of violation of local rules and policies or rules globally accepted by Internet community on using computer resources), concerning network resources located in Armenia as well as responses to them with the aim of preventing, stopping and collecting evidences about an incident.

[20] www.cert.am

CERT-AM's mission[21] is to contribute to the security of the ICT infrastructure of all Armenian institutions, bodies and agencies ('the constituents') by helping to prevent, detect, mitigate and respond to cyber-attacks and by acting as the cyber-security information exchange and incident response coordination hub for the constituents. The scope of CERT-AM's activities covers prevention, detection, response and recovery.

CERT-AM will operate according to the following key values:

- Highest standards of ethical integrity;
- High degree of service orientation and operational readiness;
- Effective responsiveness in case of incidents and emergencies and maximum commitment to resolve the issues;
- Building on, and complementing the existing capabilities in the constituents;
- Facilitating the exchange of good practices between constituents and peers;
- Fostering a culture of openness within a protected environment, operating on a need-to-know basis.

The CERT-AM it is not listed on ENISA interactive maps of CERT and is not a FIRST member[22]. On the GEANT site, organisation that is consisted of representatives from research and education network, it can be found that ASNET-AM is cyber security structure-type CERT of the Institute for Informatics and Automation Problems[23].

3.1.3 Interagency and public/private cooperation

Understanding that effective public-private cooperation, beyond strict adherence to legal requirements, is also a trust-building exercise extending beyond the letter of the law. Recognizing the need for informal but highly practical cooperation is of key importance.

CERT.AM/AM NREN CSIRT also serve as a contact points for users who need assistance in dealing with ISPs and Armenian official bodies which are in charge for investigating cybercrime and cyber-enabled offences. CERT AM/AM NREN CSIRT guarantees confidentiality of the received information about incidents.

At the moment, there are not private CERT/CSIRTs operating in Armenia. There is, however, cooperation with IT experts from private companies representing local and global/regional industries. Sometimes private sector experts provide expertise and advice to the LEA officers, but in informal format, based on personal relations and not within established cooperation framework.

In terms of other types of public-private dialogue, private sector stakeholders are invited on an occasional basis to the Parliament's relevant committees in order to provide their inputs. There is no established forum with regular meetings to exchange information on problems in cybersecurity. Instead meetings are organized on a case by case basis.

The Government is interested in working with the private companies, in particular for the Digital Armenia 10-year plan on providing a unified approach to government services. There is interest to work internationally with the private sector abroad because of the international aspects of cybersecurity.

There is a reported willingness of the Government agencies to include the representatives of the private sector in the development of the Cybersecurity Strategy of the country, which would be a welcome development in terms of public-private cooperation.

[21] https://www.cert.am/rfc2350-CERT-AM.pdf

[22] https://www.first.org/members/map

[23]https://www.geant.org/Resources/Documents/Compendium%20Layout%20ONLINE.pdf#search=CERT%20AM

3.2 Cybercrime

3.2.1 Policy framework

Armenia currently has no dedicated strategy or action plan on cybercrime as such in place or in development. The Armenian law enforcement bases all their activities related to cybercrime on criminal legislation. While substantive offences are mostly in place, there are significant gaps in terms of implementing procedural powers under the Budapest Convention on Cybercrime.

Armenia signed the Budapest Convention on Cybercrime (ETS 185) on 23 November 2001 and ratified it on 12 October 2006. Armenia is a Party as from 1 February 2007.

Armenia has initiated comprehensive reform of its criminal procedure legislation several years ago (the start of formal process dating back to 2009). The draft Code of Criminal Procedure now seems to be at the final stages of approval by a Working Group of experts at the Ministry of Justice and is expected to be submitted for parliamentary hearings in autumn 2017. The draft Code would lead to closer implementation of the relevant provisions of the Budapest Convention. The Council of Europe – through the Cybercrime@EaP projects – reviewed the draft in May 2017 and presented recommendations for refining cybercrime-related provisions.

3.2.2 Institutional framework

The Division for Combating High-Tech Crime under the General Department on Combating Organized Crime at the Police of the Republic of Armenia is a centralized unit which is responsible for handling cybercrime with country-wide competency. The police have 10 days to determine the facts and the legal basis for the investigation and then deciding either to close the matter, send the case to local police where evidence or a perpetrator is located, or to transfer the matter to the Investigative Committee. Thus, the Division is the primary police unit handling cybercrime cases at the preliminary stage (before an official investigation is opened by the Investigative Committee) and providing support to local units.

There are 8 officers employed at the Division for Combating High-Tech Crime of Armenian police. There are no specialised local units; where necessary, additional resources of the Organized Crime Department are used (either at the local offices or the headquarters). The Division is competent to investigate offences committed against computer systems such as hacking, attacks on the critical infrastructure, illegal interception and data interference. The Division is also competent to deal with offences involving technology such as computer related fraud, Internet crimes, offences involving the abuse of children, intellectual property offences as well as racism and xenophobia.

Since the reform of the criminal procedure in 2011, 95% of the criminal cases in Armenia are investigated by the Investigative Committee of the Republic of Armenia, the remaining cases being handled by specialized units for tax and customs fraud or investigations into public officials. The Committee has 6 investigators on staff dedicated to cybercrime cases. The investigator files the criminal case with the prosecutor and leads the investigative procedure. The Committee does not operate computer forensics laboratory, but instead makes use of external expertise for the analysis of electronic evidence.

Where an expert evaluation is necessary, it is performed at specialised centres, in particular the National Bureau of Expert Evaluation that is a state non-commercial centre of Armenia's Academy of Sciences.

3.2.3 International cooperation

In terms of police-to-police cooperation, the Division for Combating High-Tech Crime under the General Department on Combating Organized Crime at the Police of the Republic of Armenia, processes requests for police-to-police cooperation under the Budapest Convention and the G7 networks on 24/7 contact points. It processes only operative and intelligence information (cannot be used as evidence in criminal proceedings) and does not receive and process mutual legal assistance requests. Information received through the 24/7 point of contact is forwarded to competent investigative authorities; if the specific investigative action is required, referral is done through the Prosecutor's Office. Technical assistance and support and advice can be provided by the 24/7 point of contact.

Armenian authorities also made a decision to establish a second point of contact at the Investigative Committee of Armenia, with a request communicated to the Council of Europe in 2018. In case of either unit, there is no specific legislation establishing or providing regulations for the work of 24/7 point of contact.

At the stage of pre-trial investigation, the competent authority for mutual legal assistance is the Department for International Cooperation and Legal Support at the Prosecutor General's Office. According to the authorities, a prerequisite for request at this stage is the Red Notice / Diffusion Notice (circulated by Interpol) Reciprocity is also a prerequisite – written confirmation from the requesting state is necessary.

At the trial stage, the Ministry of Justice (Department for International Legal Assistance) is in charge of the MLA process. A prerequisite for the request is the Red Notice by Interpol / Diffusion Notice (attached to request). Request according to the European Convention on Extradition of 1957 should be supported by documents noted in Article 12 Budapest Convention. In general, an indication of clear legal basis for the request is necessary; otherwise, reciprocity is a prerequisite – in the form of express written assurance of reciprocity from the requesting State.

Armenia's current practice of international cooperation on cybercrime and electronic evidence is consistent with general practice of the Eastern Partnership states, with regard to problems as well:

- Incoming or outgoing international preservation requests (Article 29 Budapest Convention) are often not followed by mutual legal assistance requests for the production of data;
- No formal modalities for informing States requesting preservation of a necessity of mutual legal assistance request (in the best practice of the states implementing the Convention, such replies can be automated);
- Time-frames for processing and execution of incoming mutual legal assistance requests are rather long and delays are experienced mostly due to large requests requiring translation (considered to be particularly problematic) and/or need to clarify ambiguities in cases of incomplete/low-quality requests.
- Triage of mutual legal assistance requests not performed or based upon informal criteria and is not uniform in application.
- Lack of sufficiently clear and proper basis in national law to cooperate directly with multinational service providers (MSPs) in criminal cases, being one of the major reasons for declining cooperation.

3.2.4 Public/private cooperation

On 23 November 2015 the Investigative Committee signed a Memorandum of Understanding with ArmenTel, K-Telecom, UCom, Orange Armenia with the intention of workload reduction and human resources saving.

The main intentions of the Memorandum are: to take effective joint measures in the direction of operative transmission of court decisions and transcripts, and to develop the mutual cooperation on introduction of technical capabilities. In this framework, parties agreed to communicate on a standardized manner (including cover letters, electronic signatures) and agreed to cooperate in solving issues as soon as possible in case of such procedures. Furthermore, the signing providers agreed to process electronic transmission of the Investigative Committee within a short period of time and also to execute expeditiously court decisions which are designated as "urgent". A second objective of the Memorandum is to ensure that Internet Access Providers retain traffic data of their users for a period of time. Currently Armenia has no data retention legislation.

There are no immediate plans to expand the memorandum to include more companies or additional sectors such as payment processors or banks. The latter are reported to have very limited cooperation with the law enforcement. The concept of "bank secret" is invoked frequently to deny the requests for cooperation.

Academic institutions play an active role in education on cybercrime; moreover, they also support the work of the police on an occasional basis. Regarding the education mechanism between the public and the private sector both Microsoft and CISCO are regularly providing cooperation or attending forums to support the authorities with the latest developments in the topic.

Police supports state owned television programs which focus criminal topics also on cybercrime in order to raise public awareness. Private television stations also broadcast programs which are raising awareness on cybercrime. Schools regularly receive education classes by police on the topic.

All stakeholders agree, to a more or less uniform extent, that that Armenia should pursue the following elements necessary for public-private cooperation to work:

- Clear legislation setting out the procedures and rules for access to data held by Internet service providers, based on the standards of the Budapest Convention;
- Identification and engagement of all possible parties – governmental, non-governmental and business – into the multi-stakeholder process of cooperation;
- Building understanding of common interest and values for security of Armenian citizens in cyberspace and facilitating voluntary compliance to best practices (e.g. reporting, training, awareness, prevention, etc.);
- Ensure that cooperation with foreign/multinational Internet service providers follows standards and work set by the Cybercrime Convention Committee of the Council of Europe;
- Armenia should consider expanding the existing memorandum of cooperation between the Investigative Committee and telecom service providers to include more topics, scope and possible partners (e.g. the National Police);
- Encouraging the private cyber security structures to be set up (private CERTs, CSIRT) could be useful filling the gaps in expertise of the public institutions caused by the difficulty of maintaining good experts, as the offer on the private market is substantially superior.

3.2.5 Reporting mechanisms

The state owned company E-KENG provides centralized e-governance services (ex: electronic applications for visas, e-health, etc.) in the Republic of Armenia. The company operates a platform for these services and also hosts the majority of databases. If interference, leakage or irregular activities are noticed, the companies have to report it, stop the access to the system and notify this to the Data Protection Agency and the Police. Draft general directives for data protection, once approved and implemented, envisage sanctions to be applied for failure to comply.

Also, any legal entity or person can make a complaint to the police, to any police officer who is obliged to receive and register the case. Complaint can also be directly delivered to the cyber crime unit by email. In case of cybercrime reporting, the complaint is sent to General Prosecutor's Office where specialised prosecutors for cybercrime are working (two of them currently). When a criminal case is formally open, it is transferred to the Investigative Committee.

3.3 Armenia summary

Assessment item	**Republic of Armenia**
Cybersecurity	
Cybersecurity strategy in place	At drafting stage
Preventing cybercrime as a key objective of the strategy	n/a
Establishment of computer emergency response team(s), CERTs	Yes (non-governmental only)
Cooperation on both national and international level	Present
Cooperation with private sector	Present
Cybercrime	
Cybercrime strategy in place	No
Specialized cybercrime units	In place
International cooperation	In place
Public/private cooperation	Cooperation agreement
Establishment of platforms for reporting cybercrime	No

4 Azerbaijan

Data removed at request of Azerbaijani authorities

5 Republic of Belarus

5.1 Cybersecurity

5.1.1 Policy framework

There is no dedicated strategy or other specific policy document on cybersecurity currently available or being developed in Belarus.

The National Security Concept of Belarus, approved by Decree No. 575 of the President of Belarus on 09.11.2010, defines information security as a condition to protect the balanced interests of the individual, society and the State from external and internal threats related to information and identifies information security as an independent component of national security.

5.1.2 Institutional framework

Belarus has a national CERT: CERT.BY. CERT.BY is established within the structure of the Operational and Analytical Centre under the Aegis of the President of the Republic of Belarus (OAC). The main task of the Centre is to reduce threats to information security within Belarus; CERT.BY also carries out accumulation, storage and handling of statistic data related to malware dissemination and network attacks on the territory of the Republic of Belarus, as well as incidents response in the informational systems of the state agencies and organizations. The team also responds to incidents affecting information systems of the subjects of the national segment of the Internet addressed to CERT.BY independently.[24]

A Financial CERT is being created and is expected to become operational in the near future. This CERT will facilitate exchange of intelligence. In the financial sector, all incidents are to be reported to the National Bank (financial supervisor).

5.1.3 Interagency and public/private cooperation

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Belarus.

However, outside the scope of formal investigations, information exchange takes place, in various fora. For example, the financial sector has frequent meetings, organized by the National Bank, where threats and security are discussed.

Cooperation also takes place informally in the case of (security) incidents. For this purpose a secure platform is in existence that enables secure communications between mobile providers and government entities. These communications are subject to strict regulations regarding the privacy and security of the information.

The Internet Governance Forum is held in Minsk since 2016, giving opportunity to private sector, the NGOs, the academia and the public sector representatives to meet and share their views on current trends and challenges. The forum is also supported by ICANN.

As a related recent development, the Law on Public and Private Cooperation Regarding Infrastructure Development was adopted in 2015. The main principles of this act are rule of law, effectiveness of public-private partnerships, the priority of public interest and publicity. It also focuses on technical resources and infrastructure development.

[24] https://cert.by/

5.2 Cybercrime

5.2.1 Policy framework

There is no national cybercrime strategy in Belarus. Chapter 31 of the Criminal Code deals with cybercrime offences. While substantive cybercrime offences are mostly in place, there are significant gaps in terms of implementing procedural powers under the Budapest Convention on Cybercrime.

Other legislation is in place to regulate Internet service providers and data retention. Decree 129 of 2010 on cooperation between telecommunications providers and law enforcement authorities defines the retention period of subscriber information for 5 years and the competent authorities that have access to such information.

Belarus has not yet acceded to the Budapest Convention on Cybercrime (ETS 185) but has expressed a strong interest in accession.

5.2.2 Institutional framework

Since 2002, there is a High-Tech Crime Department within the Ministry of Interior of Belarus (Department "K") whose competency is to detect and deal with crimes against information security, embezzlement by means of computers, including that conducted by means of stolen and forged bank cards or their details, and to counter the distribution and advertising of child pornography on the Internet. Besides preliminary investigations, the Department "K" also assists other units across the country in matters of cybercrime and electronic evidence. There are currently 25 officers at the headquarters of Department "K".

In five regional centres of Belarus, territorial units have been established to counter hi-tech crime. The average staffing of units is 7 persons.

Since 2012, there is also a specialised unit within the Investigative Committee of the Republic of Belarus, that is, High Tech Crime and Intellectual Property Department; its function is to initiate criminal proceedings and conduct full investigations of detected criminal activities. It now employs about 30 officers dedicated to cybercrime/high-tech investigations, out of which 10 are located at headquarters.

When a more thorough examination of evidence or electronic media is required, an examination by a computer or other specialised expert can be organized. Such expert examination is the competency of qualified experts of the Forensic Centre of the Ministry of Interior of Belarus. Due to backlogs, several law enforcement units also have their own forensic capability, in order to serve investigations more directly and take evidence on site. The cybercrime unit uses technical tools and procedure that guarantee the integrity of evidence seized. The forensics centre does more in-depth forensic analysis.

Once information of a financial crime is received by the General Prosecutors Office, (GPO), depending on the scale of the infringement a criminal case is opened. The Financial Investigation is then conducted by a specialized financial investigation unit. Financial investigations and the predicate investigation are separate, and have a different mandate.

The financial investigation unit mainly prosecutes AML, tax evasion and purely financial crime.

5.2.3 International cooperation

The national authority for the 24/7 point of contact is the High-Tech Crime Department within the Ministry of Interior of Belarus (Department "K"). Since 2008, Belarus belongs to the international network of contact points established under the G7 Rome–Lyon Group. They have observed improvements with US multinational ISPs. Data preservation is requested frequently and replies are given within 10 days. The response rate has improved significantly over recent months. Law enforcement of Belarus has recently taken part in the international Cobalt/Carbanak investigation.

At the pre-trial stage of criminal proceedings, Office of the Prosecutor General of the Republic of Belarus, International Legal Department is deemed to be central authority for mutual legal assistance in criminal cases based on the principle of reciprocity. At the trial stage of criminal proceedings, the competent authorities are the International Legal Department of the Office of the Prosecutor General and the Supreme Court of the Republic of Belarus; the latter is competent only for submitting procedural or other documents in criminal cases under trial and execution of sentences (and also in relation to other decisions of the court in criminal proceedings).

Requests for legal assistance mostly concern Commonwealth of Independent States (CIS) countries. Cooperation, otherwise, takes place with the Baltic States, Poland and Germany. Recent initiatives were undertaken to improve cooperation with the US Department of Justice (DoJ). A special mailbox was set up and used for requests. The process/response time was significantly improved by this procedure (usually 1 month).

There is no treaty with the US, but cooperation takes place on the basis of reciprocity. The same goes for many individual (EU) countries. With Germany there is good cooperation with MLA and extradition on this basis.

Cooperation with Russia can incur delays, although it is not clear why. Direct cooperation with foreign counterparts can expedite this, it is observed. In most cases information and requests are sent by email, and followed up by paper copies. The resources of the national bureau of Interpol in Belarus are often used as well. The 'K' Department also cooperates with foreign law enforcement in the form of joint international operations against cybercrime, in particular in the field of child abuse online and card fraud.

Current practice of international cooperation on cybercrime and electronic evidence in Belarus is mostly consistent with general practice of the Eastern Partnership states, including with regard to problems as well:

- Incoming or outgoing international preservation requests (Article 29 Budapest Convention) are often not followed by mutual legal assistance requests for the production of data;
- No formal modalities for informing States requesting preservation of a necessity of mutual legal assistance request (in the best practice of the states implementing the Convention, such replies can be automated);
- Time-frames for processing and execution of incoming mutual legal assistance requests are rather long and delays are experienced mostly due to large requests requiring translation (considered to be particularly problematic) and/or need to clarify ambiguities in cases of incomplete/low-quality requests;
- Triage of mutual legal assistance requests not performed or based upon informal criteria and is not uniform in application;
- Lack of sufficiently clear and proper basis in national law to cooperate directly with multinational service providers (MSPs) in criminal cases, being one of the major reasons for declining cooperation.

5.2.4 Public/private cooperation

The Ministry of Interior cybercrime unit cooperates with the private sector (ISPs, banking industry). Relevant information is shared frequently. Under the regime of the special operative and search law, there are identified contact persons in place. Response times are very short; a reply within an hour is not unusual. Decree 60 of the President of Belarus from 2010 provides an umbrella/framework for this cooperation, as well as the Law on Cooperation.

There is a Memorandum of Understanding (MoU) between the investigative committee and the (around 150) ISPs in Belarus. The document is used actively, and improvements are considered. Cooperation takes place on the basis of legislation, while the MoU only sets out contact persons, procedures and clarifies technical details. It is possible to sanction entities which do not comply with requests and there have been cases where sanctions were applied.

The banking sector, the law enforcement authorities, the Ministry of Interior, Investigative Committee and the General Prosecutor's Office regularly organize round tables and conferences on cybercrime issues, which resulted in another Memorandum of Understanding by the parties related to financial crime.

Educational sessions are being regularly held by the Academic Society for law enforcement agency members and civil servants as well. Regular education is also being provided in the framework of the Ministry of Interior's Academy and it is also supported by the Minsk University. The next step for educational programs is to focus on the judiciary bodies.

Although Belarus law enforcement is allowed to request information from foreign entities and use any obtained replies as evidence at trial, the opposite is not possible. Belarusian ISPs, when they receive requests for information from abroad, have to reject these as any evidence provided abroad has to go through the national legal process for disclosure.

5.2.5 Reporting mechanisms

Cybercrime can be reported at the Ministry of Interior (including the High-tech Crime Unit). Reporting is centred on police. The roadmap currently under construction, will address further mechanisms for reporting and detection of these cases.

The Prosecutor General's Office maintains a website which facilitates online reporting of all types of crime. There is also an (anonymous) telephone hotline for the purpose of crime reporting. Several law enforcement bodies also offer this possibility on their respective websites. Security incidents can be reported at the National CERT.

Reporting is not a requirement for the police to initiate an investigation. Mere intelligence is enough to start an investigation. The police frequently receive intelligence from foreign counterparts through their 24/7 contact point.

Industry has employees dealing with handling abuse complaints, who can also be used as a first point of contact. Child abuse material related complaints are forwarded to the law enforcement.

5.3 Belarus summary

Assessment item	Republic of Belarus
Cybersecurity	
Cybersecurity strategy in place	No
Preventing cybercrime as a key objective of the strategy	n/a
Establishment of computer emergency response team(s), CERTs	Yes
Cooperation on both national and international level	Present
Cooperation with private sector	Present
Cybercrime	
Cybercrime strategy in place	No
Specialized cybercrime units	In place
International cooperation	In place
Public/private cooperation	Cooperation agreement
Establishment of platforms for reporting cybercrime	Several options

6 Georgia

6.1 Cybersecurity

6.1.1 Policy framework

The Government of Georgia has published its second Cybersecurity strategy[25], covering the period 2016 to 2018. The strategy is the key document defining state policy in the area of cybersecurity, reflecting strategic objectives, key principles, tasks and relevant activities for the fulfilment of the tasks. Moreover, the strategy, considers the key directions of the national security defined under the "Threats Assessment Document of Georgia 2015-2018" and "National Security Concept", aims at eradication and mitigation of threats identified in these documents. Ownership of the strategy is vested in the Data Exchange Agency (DEA).

The initial Cybersecurity Strategy, adopted in May 2013, has significantly supported the sustainability of cybersecurity system in Georgia, as the absolute majority of activities defined under the action plan of the abovementioned document have been fulfilled. Accordingly, the current strategy is oriented towards further development of cybersecurity area, unlike the first Strategy, which was aimed at creating general framework for the development of cybersecurity sector. Moreover, the significant novelty offered by the present Strategy is the reflection of issues related to the cyber self-defense, in the document, with the purpose of further developing the area under discussion.

Georgia has been subject to a number of cyber attacks in the past years. The cybersecurity strategy identifies the Russian Federation as a key player in the primary threats to the Georgian critical infrastructure, and considers the threat is greater than in 2008 for the following reasons:

- The Russian Federation has not changed its aggressive policy in the cyber-domain;
- During the recent years the Russian Federation has significantly enhanced its capabilities in the area of cyber-attacks;
- Russian Federation has significantly improved the specific features of application of cyber-means in the operations of psychological influence implemented by Russia;
- Since 2008, the dependence of Georgia on informational and communication technologies has significantly increased, potentially increasing the scales of anticipated damage in case of cyber-attacks.

The categories of threat identified in the strategy include:

- Cyber War;
- Cyberterrorism;
- Cyberintelligence activities; and
- Other activates directed against Georgia using cyberspace.

The key objectives and principles of the strategy incorporate the following, which are articulated in the document:

- Cybersecurity as the integral part of the national security
- Uncompromised protection and respect for the human rights and basic freedoms
- Common approach of the Government of Georgia
- Collaboration between the state and private sectors
- Active international cooperation
- Individual responsibility

[25] http://csbd.gov.ge/doc/Cybersecurity%20Strategy_eng.pdf

- Adequate measures

The key directions of the Georgian cybersecurity are provided below:

- Research and analysis;
- New legislative-normative framework;
- Enhancement of capabilities in the field of cybersecurity;
- Improved public awareness and establishment of educational base;
- International cooperation.

The proposed activities to support the strategy are set out clearly in the document.

The Data Exchange Agency (DEA) is responsible for information security and cybersecurity coordination. However, the legal basis for its actions to supervise and audit information systems in both public and private sector, is not in place as the current governmental decree addresses only state agencies as critical information infrastructure subjects.

6.1.2 Institutional framework

There are two active CERTs[26] present in Georgia:

- CERT-GE[27]: Research and Education CERT;
- CERT-GOV-GE[28]: Government CERT;

The CERT-GE has been established under the Georgian Research and Educational Networking Association (GRENA) an organization founded for the development of Information Technologies (IT) in education and research field. The founders of association GRENA are five major universities, Georgian National Academy of Science and Open Society-Georgia Foundation. Its current security services are limited to mail analysis, although CERT-GE is active in research and outreach regarding cybersecurity.

CERT.GOV.GE operates under Data Exchange Agency of the Ministry of Justice of Georgia and is responsible of handling critical incidents that occur within Georgian Governmental Networks and critical infrastructure. CERT.GOV.GE started its operations in January, 2011. CERT.GOV.GE handles all critical computer incidents, which occur in the country, in its capacity as a national CERT. The CERT.GOV.GE provides a variety of services and platforms for identifying, registering and analyzing critical computer incidents, as well as minimizing critical computer incidents throughout the country, and plays a significant role in rising the awareness of information security issues within the country.

Besides these two CSIRTs, the Ministry of Defence of Georgia established its own Cyber Security Bureau in 2014, which acts as military/defence CERT in relation to defence-related critical infrastructure. This unit has been established under the Georgian Law on Information Security.

6.1.3 Interagency and public/private cooperation

A major part of the critical informational infrastructure of Georgia is in the hands of the private sector and experience and knowledge existing in this sector is mainly accumulated within the private companies. Based on the abovementioned, it is important to develop cooperation mechanisms, which will facilitate, on the one hand, uninterrupted functioning of critical

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

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

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

informational infrastructures, and on the other hand, will become additional stimulating factor for the economic development.

Based on the Cyber Security Strategy, the Government of Georgia carries out activities which facilitate secure functioning of state bodies, private sector and civil society in cyberspace, as well as safe use of information and communication technologies and uninterrupted operation of economy and business in the country.

Georgia has a Law of Georgia on Information Security[29] which names the national CERT (CERT.GOV.GE) as the unit to which cyber incidents within Critical Infrastructure must be reported (Article 10).

The Data Exchange Agency of the Ministry of Justice has started several initiatives to coordinate cybersecurity cooperation between different stakeholders. Data Exchange Agency regularly holds the Cyber Security Forum of Georgia, which was launched in September 2012. It has 3 major tasks: identify leaders in private sector, develop management crisis scenarios and prepare for collaboration in time of crisis. It has also brought together key cyber security experts from public and private sector and has contact points in all participating organizations and other entities.

Technical requirements for security are applicable to all critical infrastructure subjects. The Law of Georgia on Information Security[30], 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 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."

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

- Creation of educational and public awareness raising programs in the field of cybersecurity;
- Capacity building of higher education system in the fields of cyber and information security;
- Training of staff and technical personnel of critical information infrastructure bodies and other interested organizations, with the objective of studying international and national standards in the field of informational security;
- Specialized trainings in investigation of cyber-incidents directed against the Georgian national security;
- Facilitation of scientific research projects in the field of cybersecurity.

There is an online Moodle platform with different level cybersecurity courses. It has exercises and a certification programme. It is co-shared with the Ministry of Defence. CERT experts have trained prosecutors on cybersecurity. There are many other initiatives in training and information.

Internships in CERT are possible to create a pool of young people who have been trained in the Data Exchange Agency. Public and private sectors share information with each other at the Georgian IT Innovations Conference (GITI).

For CERT, they have different initiatives on cyberbullying and public awareness for schools and academia. They have also delivered TV tips with advice on how to behave. They have issued

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

cybersecurity calendars and other similar things. CERT.GOV.GE also holds the annual cyber exercise and Cyber-Olympiad for specific sectors and youth.

A separate MOU exists between the Data Exchange Agency and the Association of Small and Medium ISPs. It covers assistance and threat/information sharing in the broad area of security.

6.2 Cybercrime

6.2.1 Policy framework

Although Georgia lacks a standalone cybercrime strategy, save in the more general context of cybersecurity as just noted, its first Organized Crime Strategy (2013 – 2014) specifically addressed cybercrime in Chapter III:

- 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.

The current Organized Crime Strategy (2017-2020) continues its strong focus on cybercrime in Chapter 3 of the document. It pursues the following goals:

- **Raising public awareness**: Informing the public on cybercrime and its effects, preparation of information campaigns on social networks and websites of relevant departments, preparation of public service announcements; information exchange meetings by law enforcement agencies about cybercrime and its effects;
- **Improving legislation**: Periodical revision of the legislative basis of the fight against cybercrime and, if necessary, proposing amendments;
- **Institutional capacity building**: Develop professional skills of the staff involved in the fight against cybercrime, organize trainings and study visits; development of the material and technical base of the agencies involved in the fight against cybercrime; holding meetings between the agencies involved in the fight against cybercrime; deepening of cooperation between the critical infrastructure subjects and holding meetings.

The Action Plan for the Strategy (currently covering only 2017 and 2018) involves a variety of stakeholders as bearers of responsibility for implementation, such as the Government as a whole, Prosecution Service, Ministry of Interior, Ministry of Justice and other actors.

On more operational level, Standard Operational Procedures on initial handling and further forensics of digital evidence have been prepared based on T-CY Guidelines. The SOP is for guidance only and is considered confidential and not available to the defence in any criminal trial.

The Cybercrime@EaP project held series of meetings in 2018 which discussed the need for a more inclusive and wider national cybercrime strategy, and identified a key group of participants in any development process. These include:

- Prosecutors Office
- Ministry of Justice
- Criminal Police responsible for cybercrime
- Date Protection Office
- CERTs (including MOD Cybersecurity Bureau)
- State Security Service

- Financial Investigators
- National Banks /Financial Institutions/FIU
- Public Defender /Ombudsman
- Georgian National Communications Commission
- ISP's and Telco's
- Interested NGO's
- International expertise.

6.2.2 Institutional framework

The separation of investigative jurisdiction in Georgia is regulated under Decree 178 of the Minister of Justice of Georgia. The document underlines that the investigative jurisdiction in general is vested in the investigative agencies of the Ministry of Internal Affairs, with some exceptions specifically listed in the Decree (such as crimes investigated by Investigative Division of the Ministry of Finance of Georgia).

Cyber Crime Division of the Central Criminal Police Department at the Ministry of Internal Affairs of Georgia was established by the decree of the Minister of the Interior in December 2012. Currently, there are 15 detective-investigators within the Division who are responsible for investigation of cybercrime. The Division is competent to investigate cybercrime offences in narrow sense, in particular crimes provided for in Chapter 15 (Cybercrime) of the Criminal Code of Georgia; however, the Division also provides advice, guidance and technical assistance to other police units across Georgia in investigation of cybercrime and handling of electronic evidence. The forensics team of the Ministry of the Interior handles the forensic examination duties. The cybercrime unit covers all of Georgia; however, there is some regional capability to investigate these types of crimes. Other police investigative agencies may also investigate cybercrime and also investigators from the Ministry of Finance.

Following legislative reform in 2014, the Ministry of State Security has been established separate from the Ministry of the Interior. The Ministry inherited the team of former Operative-Technical Department of the Ministry of the Interior, which now acts as a cybercrime investigation team of within the Ministry. The State Security Service is responsible for the identification, prevention and eradication of activities implemented in the cyberspace and directed against the national security. Moreover, in accordance with the legislation, State Security Service represents the body, which is equipped with exclusive authority to carry out secret investigation activities in the cyberspace. The Operative Technical Department of Security Service conducts lawful interception.

There is no dedicated cybercrime prosecutorial department. The prosecutor has overall responsibility for the supervision of the criminal police. There is one dedicated prosecutor on cybercrime. Several trainings on cybercrime and electronic evidence are offered by main dept and are attended by regional prosecutors. Distribution of responsibility of prosecutors is *ad hoc,* not by law. Regionally the prosecutors look after the local investigations.

The chief prosecutor has issued an order, in 2015, recommending parallel financial investigations in any crimes involving financial gain, including cybercrime. Cybercrime is predicate offence for money laundering. It is possible to have multi agency teams and have been used. They can also use a Joint Investigation Team (JIT) as Georgia is a party to CoE MLA Convention and its II Additional Protocol. The Multi Agency Group (MAG) has an identified investigation plan for such cases, although none have yet been undertaken involving cybercrime and financial crime.

The Ministry of Interior, as noted above, has a forensic unit dealing with digital devices. The State Security Service and National Forensic Service can conduct (digital) forensics. No list of experts exists. Several agencies conduct expertise. Prosecutor asks the agency to appoint an appropriate expert for each case. The Criminal Procedure Code sets out requirements for competence of

experts. The Georgian CERT does not have digital forensics capability, other than for malware analysis.

6.2.3 International cooperation

The 24/7 National Contact Point is operating at the Cyber Crime Division of the Central Criminal Police Department at the Ministry of Internal Affairs of Georgia. A review of 24/7 unit functions, as recommended by the Council of Europe in 2016 and 2017, has been undertaken and recommendations are being implemented (e.g. the legal basis for operation of 24/7 point of contact).

In October 2013, the Parliament 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.

Georgia is a Party to the Budapest Convention on Cybercrime since 2012 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.[31]

Georgia uses a single central authority for MLA requests irrespective of the stage of proceedings, namely, the International Cooperation Unit of the Department of Legal Affairs, Office of the Chief Prosecutor at the Ministry of Justice of Georgia. Although requests can be technically transmitted via 24/7 contact point or Interpol point, they must be addressed to the central authority. There is a separate Law on International Cooperation in Criminal Matters, and Georgia is a party to a number of MLA treaties.

The cooperation levels that currently exist include:

- Police to Police Cooperation
- FIU to FIU
- The Law on Police Cooperation
- There is a Single Point of Contact (SPOC) for Multinational Service Provider (MSP) cooperation
- The MIA provides the 24/7 point of contact under Budapest Cybercrime Convention and that of the G7 network.
- Prosecution Service has relationship with Facebook with nearly 100% response rate

In contrast to other EaP countries, Georgia uses a formal triage process to decide urgency of incoming MLA requests, which allows for high speed and efficiency in responding to large number of requests. Georgia also introduced, in 2017, the legal basis in its national criminal procedure for production orders directed to multinational service providers. At the same time, it is clear that a better understanding of different functions of various international cooperation mechanisms is still needed.

Current practice of international cooperation on cybercrime and electronic evidence in Georgia is mostly consistent with general practice of the Eastern Partnership states. Delays in practice are experienced mostly due to large requests requiring translation (considered to be particularly problematic) and/or need to clarify ambiguities in cases of incomplete/low-quality requests.

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

6.2.4 Public/private cooperation

Both Cyber Security Strategy and Strategy on against Organized Crime, as well as Digital Georgia Strategy, highlight the importance of public/private cooperation.

A Memorandum of Understanding is in force between the ISPs and the law enforcement authorities since 2010, and has been updated regularly until 2015. The aim of the Memorandum is to settle the fundamental intention of the signing parties to effectively cooperate in battling cybercrimes and at the same time to pay respect to the privacy of the subscribers. 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.[32]

The Memorandum was reported as effective by public sector stakeholders, although the private sector was more of an opinion that the document works to far lesser degree than few years ago. Industry representatives were mostly not aware of the 2010 MoU that regulates the cooperation of ISPs with LEA. The MoU and its provisions were more relevant previously, when law enforcement authorities were allowed to cooperate directly with service providers. After 2013, it is not the case anymore and now all the requests need to have a court warrant, which is more time-consuming and involves more bureaucracy, while, for example, direct cooperation and use of contact points can still be useful. In this regard, the Prosecution Service intends to begin a process of revision in the near future.

In practice, in cybercrime cases the Internet industry actively cooperated, especially when it comes to addressing information requests in individual cases. Objections do exist to the extensive cooperation demanded from the Security Service (who has direct access through a path into operational databases) which seems to be an added burden on top of the case-by-case cooperation that is already ongoing. Still, on a daily basis, many providers work closely with the law enforcement. In case of cybercrime, providers in most cases are willing to report them and in this case it seems to be high level of trust between private sector and public sector.

Foreign service providers are also open for formal cooperation with the public sector in Georgia: cooperation arrangements have been discussed already with Facebook and such negotiations are expected to start in the near future with Google as well.

The Personal Data Protection Inspector’s Office initiatives are focused on prevention rather than punishment. Their work only started in 2014 when the public really didn’t understand Data Protection issues. A survey showed 83 per cent of people believed Data Protection is important but do not know how it should be dealt with. DPO have issued advice to the public and an alphabet of information.

The DPO also engage with data controllers and advice for startups. They provide free consultations to interested customers and provide sector specific recommendations.

The Prosecutors office is active in crime prevention, when prosecutors meet with the public and students with advice against particular crime types. It is criteria in the performance indicators. To date there has been nothing in relation to cybercrime but it will be in the next strategy. It is proposed to coordinate future activities with others.

When new legislation is being drafted, specific working groups are established. Private sector entities can be involved and consulted during the process. Private sector stakeholders are invited on an occasional basis to the Parliament's relevant committees in order to provide their inputs.

[32] ibíd.

6.2.5 Reporting mechanism

In relation to cybercrime, centralised crime and incident reporting are still conducted as fragmented activities, and are part of, varied efforts by differing authorities. In order to develop a coherent strategy, more use of intelligence, crime reports and other information from industry is relevant and more coordination is desirable in this area.

Examples of some of the reporting mechanisms are:

- Victims are expected to report crime to the MIA or the prosecutor's office (they send to MIA).
- The MIA has web site including email address to report crime or call 112. Also, on Prosecutors web site, reporting options exist, including a hotline and information about where to report. Cybercrime police also has email and hot line; however there is no online reporting capability or template.
- The Law of Georgia on the prevention of Money Laundering obliges entities to report. Prosecutor coordinates and investigates some listed crimes.
- AML entities have responsibility to report to FIU, who may report to the prosecutor and or financial investigators. There have been cybercrime investigations as a result of FIU disclosures.
- If the Data Protection Office receives complaint they will send to relevant authority by law, usually to MIA.
- Prosecutors and investigators (and experts) have full access to investigative information covered by CPC. All investigations, prosecutions and judgements are collected and sent to statistics agency. Continuing offences are adopted in cases where there are many offences committed by the same person.

The prosecutor's office has had some cybercrime cases, with mixed success. A total of 150 cases were dealt with in 2017. There is a larger disparity between the number of cybercrime cases and the incidents of cybersecurity, with over 10,000 of the latter reported in 2017.

In relation to child protection, a reporting hotline is being created (stopline.ge) and INHOPE membership is upcoming. Georgia is keen on using the Internet Watch Foundation (IWF) blacklist and in addition wants to involve end users to discuss if they want to use filters and provide opportunities for the end users and have hotlines. ISP could be liable for distribution of CSE once they are aware. ISP reported to police and they take a copy and then take down.

The Chief Security Officer (CSO) in private company is responsible for liaising with the police/prosecutors. Anyone in company finding any suspicious material, reports to the CSO. The company then awaits a decision from law enforcement as to takedown.

In terms of data subject rights – the Personal Data Protection Inspector's Office is accessible on any level, complaints by web; can upload breaches, or contact may be made by phone or personally. There is no legal obligation to receive reports from data breach victims, and therefore no direct way of finding out about breaches and developing useful statistics.

6.3 Georgia summary

Assessment item	Georgia
Cybersecurity	
Cybersecurity strategy in place	Yes
Preventing cybercrime as a key objective of the strategy	Yes
Establishment of computer emergency response team(s), CERTs	Yes
Cooperation on both national and international level	Present
Cooperation with private sector	Present
Cybercrime	
Cybercrime strategy in place	Yes – as part of Organized Crime Strategy
Specialized cybercrime units	In place
International cooperation	In place
Public/private cooperation	Cooperation agreement
Establishment of platforms for reporting cybercrime	Several options

7 Republic of Moldova

7.1 Cybersecurity

7.1.1 Policy framework

Draft national Programme on Ensuring Cybersecurity of the Republic of Moldova and its action plan (currently the National Programme on Cyber Security 2016-2020) is the key policy document in Moldova on the aspects of cybersecurity.

Relevant sections of the drat Programme aim to achieve safe processing, storage and access to data; security and integrity of electronic communications networks and services; capacities of prevention and emergency response (CERT); strengthening cyber defence capacities; education and information; and international cooperation and contact.

The Moldovan authorities are also guided by 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.

7.1.2 Institutional framework

Two CERTs have been established in Moldova:

- MD-CERT 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 Security CERT-GOV-MD set up within the Special Communications Centre.

RENAM network is providing services for scientific and educational organizations, personal members of scientific – educational community of Moldova. MD-CERT at RENAM is the centre of computer security incidents analysis operating as important element of the national research and educational networking infrastructure. MD-CERT is engaged in gathering, registration and analyzing of the facts of all computer incidents (i.e. attempts or the facts of infringements of the owner of the information, or various attacks within network or from the Internet) concerning network resources located on the territory of Moldova, but fist of all that are affecting users of the Research and Educational network.[33]

CERT-GOV-MD 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 strengthened and transformed into a national CERT. The mission of the Centre for Cyber Security is to support the Moldovan society in protecting against IT incidents. CERT-GOV-MD is the focal point for reporting and coordinating security incidents in communications and information systems under the management of the Special Telecommunications Centre. CERT-GOV-MD facilitates the exchange of information on IT incidents between organizations in society and disseminates information about new issues that could hinder the operation of government IT systems. At the same time, CERT-GOV-MD provides information and advice on pro-active measures, such as the compilation and completion of statistics.[34]

7.1.3 Interagency and public/private cooperation

CERT-GOV-MD initiated bilateral and multilateral cooperation with national CERTs in the area of cybersecurity.

[33] http://cert.md/

[34] https://stisc.gov.md/ro/content/cert-gov-md

As regards cybersecurity incidents, ISPs need to report to national CERT-GOV-MD, if the incident is serious. The incident can be taken further to the Police to investigate.

CERT-GOV-MD is very active in awareness and outreach, and is an essential actor in organizing Cyber Week events in Moldova, which include international Cyber Drills aimed at increasing skills of all participants, as well as serving as a forum of public-private cooperation between the government and the industry.

7.2 Cybercrime

7.2.1 Policy framework

So far, there are no dedicated strategies/action plans on cybercrime currently in force in Moldova.

However, since 2015, there is a separate section No. 4 entitled "Preventing and combating cybercrime" in the draft national Programme on Ensuring Cybersecurity of the Republic of Moldova and its action plan (currently the National Programme on Cyber Security 2016-2020). The section focuses on the further development of legislation, training of law enforcement, implementation of Council of Europe recommendations on the subject, accession to the Additional Protocol to the Budapest Convention on Cybercrime, ensuring compliance with the Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention), further regulatory framework study, and further strengthening of capacitates of authorities tasked with preventing and combating cybercrime.

The Cybercrime Programme Office of the Council of Europe was asked to provide corresponding expertise and has engaged the experts to provide comments on the draft Programme in November 2015.

Certain elements of fight against cybercrime are also covered by the Information Security Concept and National Strategy for Information Society Development - Digital Moldova 2020 and the Action Plan on its implementation; for example:

- 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

Moldova has signed the Budapest Convention on Cybercrime (ETS 185) on 23 November 2001, ratified it on 12 May 2009 and it entered into force on 1 September 2009.

7.2.2 Institutional framework

The Centre for Combating Cybercrime at the National Inspectorate for Investigations of the General Inspectorate of Police of the Ministry of the Interior of Moldova is the primary unit for the investigation of cybercrime. The Centre currently employs 29 officers (7 criminal investigative officers and 22 investigative officers) tasked with preliminary investigative and operative-detective activities in terms of cybercrime offences. Similar to other jurisdictions, the Centre is active in providing assistance and guidance to local police units in cybercrime and electronic evidence matters.

The work of the Centre is supported by a cyber lab created within the Technical Criminalist Directorate of the Ministry of Internal Affairs, where technical specialists work on analyses, collection and processing of electronic evidence. The process of forensic examinations takes place

in compliance with the provisions of the Criminal Code, Criminal Procedure Code, methodological materials and other applicable standards.

Since 2010, an Information Technology and Cyber Crime Investigation Section as an independent structural subdivision of the Prosecutor General's Office directly under the General Prosecutor, is in charge of criminal investigations and prosecutions in cybercrime cases. There are currently 5 prosecutors in the section, supported by 4 consultants and 2 IT specialists, who are tasked the investigation of the full spectrum of offences provided by Article 2-10 Budapest Convention, as well as related offences against or with use of computer systems and data.

Both the Ministry of Interior and the General Prosecutor's Office can receive and process crime reports from individuals, legal entities and state authorities directly. Due to daily interaction between these institutions and supervision by specialized prosecutors of all relevant investigations, coordination is considered to be efficient.

7.2.3 International cooperation

Moldova employs not one but two competent 24/7 points of contact for the purposes of the Budapest Convention, one at the General Police Inspectorate (Centre for Combating Cybercrime of National Inspectorate for Investigations) of the Ministry of the Interior and another at the Prosecutor General's Office (Information Technology and Cyber Crime Investigation Section). This in general is considered to be an efficient setup.

The 24/7 point of contact at the General Police Inspectorate provides police-to-police cooperation under the Budapest Convention and the network of the G7, processing only operative and intelligence information (cannot be used as evidence in criminal proceedings). It does not receive and process mutual legal assistance requests, but can provide technical assistance and support/advice.

The Department for International Legal Assistance of the Prosecutor General's Office of the Republic of Moldova is the designated central authority for mutual legal assistance at the stage of pre-trial investigation. Requests at the stage of trial proceedings or sentence execution are dealt with by the Ministry of Justice, International Legal Cooperation Division. INTERPOL National Contact Point can receive but not implement the MLA request and has to send it to the competent authority for action.

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[35].

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.[36]

Moldova's current practice of international cooperation on cybercrime and electronic evidence is consistent with general practice of the Eastern Partnership states, with regard to problems as well:

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

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

- Incoming or outgoing international preservation requests (Article 29 Budapest Convention) are often not followed by mutual legal assistance requests for the production of data;
- No formal modalities for informing States requesting preservation of a necessity of mutual legal assistance request (in the best practice of the states implementing the Convention, such replies can be automated);
- Time-frames for processing and execution of incoming mutual legal assistance requests are rather long and delays are experienced mostly due to large requests requiring translation (considered to be particularly problematic) and/or need to clarify ambiguities in cases of incomplete/low-quality requests;
- Triage of mutual legal assistance requests not performed or based upon informal criteria and is not uniform in application;
- Lack of sufficiently clear and proper basis in national law to cooperate directly with multinational service providers (MSPs) in criminal cases, being one of the major reasons for declining cooperation.

Although Moldovan authorities have good cooperation with other countries, these options are often underused. There have been successful international investigations and uses of Joint Investigation Teams as well as cooperation with international organizations such as CIS Bureau for police cooperation and SELEC.

There is also some cooperation with Multinational Service Providers, but often requests have been refused.

7.2.4 Public/private cooperation

There is no general Memorandum of Understanding between the ISPs and the public sector. Such an approach was discussed in 2012-2013, however it never received a mutual recognition and neither did it arrive to a final drafting phase. Efforts to re-discuss this approach in 2015 and 2018, initiated by the National Cybercrime Investigations Centre, Prosecutor General's Office and the Council of Europe, while successful in bringing stakeholders onboard, were not followed up with any specific text.

An important issue is that any information gathered from private parties following voluntary co-operation can only be used as intelligence. Whilst it can be used to motivate the use of police powers, it cannot be used as evidence. For it to be used as evidence the fact have to be collected through the legal process.

Similarly, a problem is that to receive information from ISPs, significant suspicion (reasonable doubt) against a subject is required for the investigative judge to authorise information gathering. This makes it hard to build cases that require information residing with an ISP and that have yet to arrive at full suspicion against a subject. It was observed that this hinders building cybercrime cases.

At the same time, the National Bank – which oversees all banks in Moldova - has concluded a Memorandum of Understanding with the General Prosecutor's Office. There is a Memorandum of Understanding between the Cybercrime Centre of Moldovan Police and CERT-MD. Cybercrime Centre has also good cooperation with entities responsible for child protection, intellectual property and copyright. Cybercrime Centre has also cooperation agreement with Ministry of Education and National Bank.

There is a Cross Agency Regulation which was signed by all law enforcement bodies in Moldova. The document is considered as normative. Its existence is public knowledge, but the content of the regulation is classified.

Moldovan ISPs cannot provide evidence directly to foreign law enforcement; however law enforcement of Moldova has shared such information with Europol and Interpol and foreign law enforcement on the basis of rogatory letters. Another obstacle to sharing information directly by an ISP to foreign law enforcement is the personal data protection that requires the transfer of personal data abroad to be authorized. However there is good cooperation between the Moldovan Prosecutor General's Office and foreign law enforcement, such as German BKA and American FBI, who have obtained interception of communications from Moldova through legal cooperation.

7.2.5 Reporting mechanisms

Reporting of crime is not mandatory unless it is a serious crime. The same applies to cybercrime. In order to encourage reporting, awareness has been raised as well as made reporting easier for the individuals and businesses.

General Prosecutors Office has established a hotline that can be used to report cybercrime.

As Cybercrime Centre has also MoU with CERT-GOV-MD, it is possible to start a criminal investigation on the basis of information shared by CERT.

7.3 Republic of Moldova summary

Assessment item	**Republic of Moldova**
Cybersecurity	
Cybersecurity strategy in place	As a draft Programme
Preventing cybercrime as a key objective of the strategy	Yes
Establishment of computer emergency response team(s), CERTs	Yes
Cooperation on both national and international level	Present
Cooperation with private sector	Present
Cybercrime	
Cybercrime strategy in place	As a part of draft Programme
Specialized cybercrime units	In place
International cooperation	In place
Public/private cooperation	Informal
Establishment of platforms for reporting cybercrime	No

8 Ukraine

8.1 Cybersecurity

8.1.1 Policy framework

During recent years Ukraine has adopted several policy instruments on cybersecurity, including Law on Basic Principles of Cybersecurity.

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.

The Cybersecurity Strategy was adopted in 2016 with the goal of creating conditions that ensure safe cyberspace and its use in the interests of individual, society and government. It is built on three major objectives:

- Developing national cybersecurity system;
- Enhancing capabilities across security and defence sector;
- Ensuring cybersecurity of critical information infrastructure and of government information resources.

The Strategy identifies the following threats:

- Cyber threats of military nature
- Cyber espionage
- Cyberterrorism
- Cybercrime

The Strategy lists the following key areas for ensuring cyber security of Ukraine:

- Development of safe, sustainable and reliable cyberspace;
- Cybersecurity of the Government electronic information resources;
- Critical infrastructure cybersecurity;
- Development of cybersecurity capacity in the defence sector;
- Fighting cybercrime

The implementation of the Strategy is built on yearly Action Plans since 2016, although the Action Plan for 2018 is still pending adoption (and is less likely to be adopted already).

There is also a Presidential Decree 32/2016 on cybersecurity that has been followed by several governmental decisions on its implementation.

Although there is already a legislative act in force (since May 2018) on the Basic Principles of Cybersecurity, additional amendments to implement the European Union Network and Information Security Directive are being prepared.

8.1.2 Institutional framework

Ukraine's CERT is the CERT-UA[37], which is the governmental CSIRT established in 2007 under the State Service of Special Communication and Information Protection of Ukraine.

[37] www.cert.gov.ua

Under the Law of Ukraine on Basic Principles of Cyber Security of Ukraine, the State Service for Special Communications and Information Protection of Ukraine:

- Formulates and implements state policy on the protection of state information resources and information in the cyberspace, the requirement for protection of which is established by law, cyber defence of objects of critical information infrastructure, and exercises state control in these areas;
- Coordinates the activities of other entities providing cyber security regarding cyber defence;
- Ensures the creation and operation of the National Telecommunication Network, implementation of the organizational and technical model of cyber defence;
- Carries out organizational and technical measures to prevent, detect and respond to cyber incidents and cyber attacks and to eliminate their consequences;
- Informs about cyber threats and appropriate methods of protection against them;
- Ensures the implementation of the audit of information security in critical infrastructure objects, sets requirements for information security auditors, and determines the procedure for their certification (re-certification);
- Coordinates, organizes and conducts audit of the security of communication and technological systems of objects of critical infrastructure for vulnerability;
- Ensures the functioning of the State Centre for Cyber Defence, the Government Response Team for Computer Emergencies in Ukraine CERT-UA.[38]

Other important players in the field of cyber security are the National Police of Ukraine, the Security Service of Ukraine, the Ministry of Defence of Ukraine and the General Staff of the Armed Forces of Ukraine, intelligence agencies, and the National Bank of Ukraine.[39]

8.1.3 Interagency and public/private cooperation

The 2016 Cybersecurity Strategy of Ukraine specifically notes that:

"An appropriate environment should be created for involvement in cyber security activities of Ukraine for some enterprises, institutions and organizations irrespective of the form of ownership and which operate in the field of electronic communications, information security and/or are owners [...] of critical infrastructure. In accordance with the law, the issues of mandatory measures for information protection and cyber defence should be settled along with assistance to state agencies in their cyber security and cyber defence tasks implementation.

The State will encourage involvement of research institutions, educational institutions, organizations, non-governmental organizations and citizens into development and implementation of measures on cyber security and cyber defence."

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.

In practice, as regards cooperation in the area of cybersecurity, cybersecurity incident handling and information exchange is largely taking place on informal basis. Cooperation is often based on the MoU or cooperation agreement, such as the agreement between Security Service of Ukraine and CERT-UA.

8.2 Cybercrime

[38] Article 8 of the Law.

[39] Ibid.

8.2.1 Policy framework

Although there is no standalone cybercrime strategy in place in Ukraine, Section 4.5 of the 2016 Cybersecurity Strategy of Ukraine envisages the following actions with specific focus on cybercrime:

- Establishment of effective and convenient contact-centre for reporting the cases of cyber crimes and fraud in cyberspace;
- Improving rapid law enforcement response to cyber crime, especially operational capabilities upgrade of regional law enforcement units;
- Improvement of procedural mechanisms for gathering of digital (electronic) criminal evidence; improving classification, techniques, means and technologies of cyber crime identification, cyber crime documentation and expert studies;
- Court-ordered blocking of the identified information resource (information service) by operators and providers of telecommunications;
- Norm-setting procedure to issue instructions, binding upon the operators and providers of telecommunications with respect to emergency recording and subsequent storage of electronic data, traffic data retention;
- Regulation of issue about urgent implementation of procedural actions in real-time environments by applying electronic documents and digital signature;
- Implementation of the scheme (protocol) for law enforcement coordination in the area of combating cyber crime;
- Training of judges (investigative judges), investigators and prosecutors for operation with electronic criminal evidence, giving full consideration to cyber crimes features;
- Introduction of special procedure for information interception in case of cyber crime investigations;
- Improving skills training of law enforcement staff.

There is no information about the Action Plan for implementation of this particular section of the Strategy, as well as any progress reporting available in this regard. The annual action plan to implement the cybersecurity strategy still identifies State Service for Special Communications and Information Protection (which hosts CERT-UA) as the main implementer.

Ukraine signed the Budapest Convention on 23 November 2001 and ratified it on 10 March 2006 with entry into on 1 July 2006. It has to be noted that while substantive offences are mostly in place, there are still significant gaps in terms of implementing procedural powers under the Budapest Convention on Cybercrime.

8.2.2 Institutional framework

Following the reform implemented in 2015, there is now a Cyber Police Department of the National Police of Ukraine, as part of the Ministry of Internal Affairs of Ukraine. The Cyber Police Department has currently only operative/intelligence functions and its officers do not conduct full investigations. It currently employs 400 officers across entire Ukraine in central unit and regional divisions across the country. With recent reform, police detectives / special agents will be added to its ranks, which should allow the National Police to conduct investigations as well.

The Department of counterintelligence protection of state's interests in sphere of information security of the State Security Service of Ukraine is another specialized law enforcement unit in Ukraine. The Department investigates crimes established by Article 359 of the Criminal Code of Ukraine (Illegal use of technical means for covert capture of information). Competencies of the Department also include investigation of crimes committed by means of computers and telecom channels established by articles 361, 361-1, 361-2, 362, 363, 363-1 of the Criminal Code of Ukraine (which correspond to offences under Articles 2-6 of the Budapest Convention).

Functions are distributed between the units of the Ministry of Interior and the Security Service of Ukraine on the basis of investigative competence regarding a relevant crime as established by Article 112 of the Criminal Procedural Code of Ukraine. In many cases, the investigative competence on such crimes can vary. Moreover, the distribution of functions is linked to the area of responsibility of the police and Security Service. For the Ministry of Interior, the key focus is to protect rights of people, companies, institutions, organizations, interests of the State and society against unlawful acts. For the State Security Service, the focus is to protect the State, its constitutional order, State security, as well as to conduct counter intelligence activities.

8.2.3 International Cooperation

As Ukraine has suffered a lot from different and large-scale cyber attacks in recent years, international cooperation has become a priority issue.

The Cyber-Police Department of the National Police of Ukraine, as part of the Ministry of Internal Affairs, performs the functions of the 24/7 point of contact. The 24/7 contact point is executing only police-to-police type of requests related to cybercrime and electronic evidence. It can provide assistance in the investigation of criminal offences connected with computer systems and exchange of operative information (that is not the evidence in criminal proceedings). The central authorities of Ukraine may take into consideration a request that came from the requesting party electronically, by facsimile or other means of communication.

Because of the absence of a mechanism for exchanging messages to/from international law-enforcement agencies between the National Police and Security Service of Ukraine, the possibility of establishing a second 24/7 contact point at the Security Service of Ukraine is being currently discussed. The additional 24/7 contact point would be based at the Department of Counterintelligence Protection of State's Interests in Sphere of Information Security, the unit of Security Service of Ukraine tasked with counteracting cyber threats and cyber terrorism.

During the stage of pre-trial investigation, the Prosecutor General's Office (Department for International Legal Cooperation) is the central authority. According to the newly adopted legislation, the National Anticorruption Bureau of Ukraine is also a central authority in execution of the MLA requests at the stage of pre-trial investigation. At the trial stage, the Ministry of Justice (Division on Mutual Legal Assistance in Criminal Matters, International Legal Cooperation Department, Directorate for International Law) is handling MLA requests.

Ukraine reports good international cooperation with USA, Germany, the Netherlands and Austria. Ukrainian authorities participated and joint investigation teams were used in Avalanche and Mozart cybercrime investigations that involved several countries. During the Avalanche operation, measures were also taken in Ukraine and searches in several cities took place. Ukraine also cooperates with Eurojust and so far several coordination meetings have been organised.

Ukraine uses also Mutual Legal Assistance tools and is sending and receiving requests from abroad. Most of the incoming requests are fulfilled. Some problems have been with regard to disclosure of data to other countries, because the lack of data retention legislative framework. Preparing requests and joint operations also require time. Executing requests received from other countries is working effectively, including obtaining domestic court warrants.

Ukraine's current practice of international cooperation on cybercrime and electronic evidence is consistent with general practice of the Eastern Partnership states, with regard to problems as well:

- Incoming or outgoing international preservation requests (Article 29 Budapest Convention) are often not followed by mutual legal assistance requests for the production of data;

- No formal modalities for informing States requesting preservation of a necessity of mutual legal assistance request (in the best practice of the states implementing the Convention, such replies can be automated);
- Time-frames for processing and execution of incoming mutual legal assistance requests are rather long and delays are experienced mostly due to large requests requiring translation (considered to be particularly problematic) and/or need to clarify ambiguities in cases of incomplete/low-quality requests;
- Triage of mutual legal assistance requests not performed or based upon informal criteria and is not uniform in application;
- Lack of sufficiently clear and proper basis in national law to cooperate directly with multinational service providers (MSPs) in criminal cases, being one of the major reasons for declining cooperation.

8.2.4 Public/private cooperation

From the perspective of the Government of Ukraine, there is an ongoing dialogue with ISPs and financial institutions taking place and cooperation agreement has been concluded between police and one ISP (Lifecell) as well as between police and financial institutions. There are also informal cooperation mechanisms that include 24/7 availability for calls and mailing lists between the points of contact. There are also police liaison officers in other government institutions that can also facilitate cooperation and information exchange.

A Memorandum of Understanding approach and a Round Table discussion group already exist, however these are not well communicated in respect of its members/drivers, procedures, responsibilities, functions and most importantly: the next steps. The Memorandum of Understanding and the Round Table are the approaches which can be the common grounds to make a move forward in Ukraine, since all stakeholders struggle from the same issues: (1) unclear legal grounds, (2) inconsequent application of law, (3) no trust towards each other and (4) cybersecurity /crime as a whole is managed differently by each elected government.

In 2017, following the series of workshops and meetings in Ukraine, the Council of Europe also suggested to both public and private sector representatives to draft a new MoU that would be based on law and that would prescribe cooperation frameworks, procedures to request and disclose data, information exchange channels including contact points and other technical details concerning everyday cooperation to fight cybercrime and ensure cyber security. The draft of the document, together with the proposed amendments to Ukraine's variety of laws, has been prepared by a group of experts in cooperation with national counterparts, and handed over to the authorities of Ukraine by the end of 2017; since then, the National Security Council took the lead of negotiating the terms of the document with both the government and the Internet industry.

In practice, all law enforcement authorities cooperate mostly with telecommunication service providers and ISPs. Cooperation includes requests for data as well as notification and take-down of illegal content. Police reported that the cooperation with the major ISPs still needs development on the part of the business.

In addition, Cyber Police cooperates often with banking institutions. The Security Service of Ukraine, whose task is also to prevent and fight serious crime, cooperates with critical infrastructure entities both in criminal investigations and cybersecurity incident investigations.

8.2.5 Reporting mechanisms

No specific cybercrime reporting takes place in Ukraine beyond the regular reporting of crime to law enforcement agencies. ISPs are generally not obliged to report where attacks do not concern critical infrastructure.

Reporting of cybercrime is overall not mandatory. However, concerning recent malware and ransomware attacks against Ukraine, around 2500 reports were received from private sector. There is an obligation for critical infrastructure objects, identified in the recently adopted Law of Ukraine on Basic Principles of Cyber Security in Ukraine, to report cyber incidents.

The reporting of cybercrime does not employ any specialized solutions, as it is a part of overall police reporting; all cases are entered into electronic Registry of Pre-Trial Investigations by investigators and prosecutors - operative officers of the Cyber Police have no right to make entries to the system.

8.3 Ukraine summary

Assessment item	**Ukraine**
Cybersecurity	
Cybersecurity strategy in place	Yes
Preventing cybercrime as a key objective of the strategy	Yes
Establishment of computer emergency response team(s), CERTs	Yes
Cooperation on both national and international level	Present
Cooperation with private sector	Informal
Cybercrime	
Cybercrime strategy in place	Yes, as part of the Cybersecurity Strategy
Specialized cybercrime units	In place
International cooperation	In place
Public/private cooperation	Informal
Establishment of platforms for reporting cybercrime	No

9 Summary table

Cybersecurity strategy	**Armenia**	**Azerbaijan**	**Belarus**	**Georgia**	**Moldova**	**Ukraine**
Cybersecurity strategy in place	At drafting stage	At drafting stage	No	Yes	As a draft Programme	Yes
Cybersecurity strategy names preventing cybercrime as a key objective	n/a	n/a	n/a	Yes	Yes	Yes
Computer emergency response team(s), CERTs	Yes (non-governmental)	Yes	Yes	Yes	Yes	Yes
Cooperation on both national and international level;	Present	Present	Present	Present	Present	Present
Cooperation with private sector	Present	Present	Present	Present	Present	Informal
Cybercrime strategy	**Armenia**	**Azerbaijan**	**Belarus**	**Georgia**	**Moldova**	**Ukraine**
Cybercrime strategy in place	No	No	No	Yes - part of Organized Crime Strategy	As a part of draft Programme	Yes, as part of the Cybersecurity Strategy
Specialized cybercrime units	In place	In place	In place	In place	In place	In place
Public/private cooperation	In place	In place	In place	In place	In place	In place
International cooperation	Cooperation agreement	Informal	Cooperation agreement	Cooperation agreement	Informal	Informal
Establishment of platforms for reporting cybercrime	No	Several options	Several options	Several options	No	No

10 Conclusions and recommendations

10.1 Conclusions

10.1.1 Status of Cybersecurity or –crime strategy

A coherent approach to the challenges of cybercrime and electronic evidence, involving key stakeholders, is required.

Georgia, Ukraine and Moldova have cybercrime strategies and/or action plans as part of other strategies:

- In Georgia, cybercrime is now covered by the updated National Strategy 2017-2020 for Combating Organised Crime and its Action Plan 2017-2018.
- In Ukraine, Section 4.5 of the Cybersecurity Strategy of Ukraine (enacted by Decree 96 of the President of Ukraine of 15 March 2016) addresses the issue of fighting cybercrime, with yearly action plans since 2016.
- Since 2015, in Moldova there is a separate section No. 4 entitled "Preventing and combating cybercrime" in the National Programme on Cybersecurity 2016-2020" (adopted by Government Decision n°811 dd. 29/10/2015). Moldovan authorities are also guided by 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.

Azerbaijan, Armenia and Belarus do not have a strategy/action plan to tackle cybercrime nor as part of another strategy.

It will be necessary to define strategic priorities on cybercrime and electronic evidence either as part of or in addition to cyber security strategies.

Under the Cybercrime@EaP project a Declaration on Strategic Priorities for the Cooperation against Cybercrime in the EaP Region was adopted by all EaP states October 2013 (Kyiv, Ukraine). Under this document, the countries committed to pursue the necessary actions in key areas, such as procedural law, safeguards and guarantees, data protection and protection of children against online sexual abuse and exploitation with the objective of adopting an overarching effective framework to combat cybercrime on the basis of the Budapest Convention. The Declaration could and perhaps should be used as source of reference for national cybercrime strategies' development.

Policies or strategies should be based on knowledge of cyber threats, problems and challenges, as well as informed decision understanding the actual threats and challenges of cyberspace. It is therefore essential to support key stakeholders in the preparation of situation reports on cybercrime and electronic evidence in their respective countries. Such reports should be the starting point of a policy making process.

10.1.2 Interagency cooperation

All Eastern Partnership countries have units specialized in the investigation of cybercrime, and some also have specialized prosecution units or specially assigned prosecutors for cybercrime matters.

However, a recurring problem for the Eastern Partnership remains the division of competences between various agencies competent to investigate cybercrime. Some EAP states have both security service and regular police/Ministry of the Interior units designated as investigative authorities for cybercrime, sometimes with competing and unclear divisions of powers or investigative jurisdiction. Beyond the reasons of efficiency and coordination, with cybercrime becoming an increasingly mainstream matter of criminal justice systems, security services do not have sufficient resources or even enough rationale to be dealing with day-to-day investigations of cybercrime offences – and, moreover, of traditional offences involving electronic evidence - that should be performed by regular investigative units of the police. Moreover, the concerns of safeguards and guarantees are also applicable in terms of procedural powers, as security services usually have a wider array of methods and powers beyond criminal procedure at their disposal, some of which may not be subject to the same or similar system of controls and conditions inherent in mainstream criminal investigations.

In some of EAP jurisdictions, the investigative powers are divided between the police units and special investigative agencies that operate beyond police/Ministry of the Interior structures. While this is primarily a regulatory and policy choice, lack of clarity remains as to the division of competencies between "preliminary" and "full" investigations performed by police forces and investigative agencies respectively. At the same time, responsibilities for international police-to-police cooperation are retained at police units rather than fully-fledged investigators who should be more competent in terms of receiving and processing such requests and have a full suite of procedural powers available to them.

On the other hand, there is almost uniform understanding of the functions of cybercrime units as supporters of other investigative units/authorities when it comes to issues of electronic evidence. Such units would provide guidance, advise and even technical expertise in cases that require handling of electronic evidence; having, in some of the EAP countries, computer forensics services directly within the structure of the same government agency and readily available to provide expert support to units in question is certainly helpful in this regard.

Some of the investigative units report particularly low number of cybercrime investigations per year (in double or even single digits in some jurisdictions), in contrast to far greater number of cyber security incidents or overall assessment of the scope of the problem, especially when the number of criminal cases with electronic evidence elements is taken into account. This points at the need to focus on greater efficiency of reporting systems and processing of cases by investigative units.

10.1.3 International cooperation and regional approach

Given the transnational nature of cybercrime and electronic evidence, effective international cooperation is essential. This includes police-to-police as well as judicial cooperation (mutual legal assistance). Key stakeholders include competent authorities within the Ministries of Justice, prosecution services and Ministries of Interior or police.

In terms of judicial cooperation, all of the Eastern Partnership States have designated authorities for mutual legal assistance. With one exception where the authority is the same for all stages of proceedings, the Office of the Prosecutor General is usually the central authority at the pre-trial stage of investigation, while the Ministry of Justice is the one for the trial stage. End-to-end procedures for the handling of incoming and outgoing mutual legal assistance requests are rather similar in Eastern Partnership countries. Differences may be due to adversarial, common law inspired criminal proceedings in some states of the region, as well as to provisional steps of compliance checking (e.g. technical pre-screening, applicability of urgency procedures) and additional management steps (e.g. processing of requests through local divisions of justice).

In order to facilitate expedited cooperation on cybercrime and electronic evidence, the Budapest Convention foresees a network of 24/7 points of contact. In most Parties contact points have been established either in the police (often specialised cybercrime units) or in specialised prosecution services or in both. Their role of contact points includes the facilitation of mutual legal assistance if they do not have the competence for mutual legal assistance themselves. Such units are available and operational in all Eastern Partnership countries.

Despite the existence of established mutual legal assistance authorities and 24/7 points of contact under Article 35 Budapest Convention in all Eastern Partnership states, the following concerns still remain:

- There are obvious gaps in legal regulations as well as practice of data preservation. Data preservation provisions of the Budapest Convention are not properly implemented in majority of the Eastern Partnership States, and general powers for production, search and seizure are used instead.

- In some of the Eastern Partnership States, subscriber information is considered to be a part of traffic data and is treated as such, thus making it difficult to obtain it without a court order.

- Incoming or outgoing international preservation requests (Article 29 Budapest Convention) are often not followed by mutual legal assistance requests for the production of data; moreover, there are often no formal modalities for informing States requesting preservation of a necessity of mutual legal assistance request (in the best practice of the states implementing the Convention, such replies can be automated).

- The need to accompany the expedited preservation of data (Articles 16 and 29 Budapest Convention) by the partial disclosure of a sufficient amount of traffic data to determine the path of a communication (Articles 17 and 30 Budapest Convention) appears to be problematic for Eastern Partnership countries due to insufficient legal regulations.

- Delays processing and execution of incoming mutual legal assistance requests are experienced mostly due to large requests requiring translation and/or need to clarify ambiguities in cases of incomplete/low-quality requests. Translation of documents and related quality checks are considered particularly problematic among Eastern Partnership States.

- Consideration of incoming mutual legal assistance as urgent or as priority, with one exception, is based upon informal criteria and is not uniform in application. Availability of formal and uniform criteria for assigning urgency to specific requests, as well as transparency in making these criteria known to international counterparts, may be considered as possible solution for handling large number of incoming requests.

- Direct contact with foreign or multinational service providers is an increasingly important concern for all Eastern Partnership States. Proper legal regulation is essential for this process, as foreign/multinational service providers do cooperate on a voluntary basis, where lack of clear and proper basis in national law could be one of the major reasons for declining cooperation.

Building on the results of the previous projects specialized on the theme of international cooperation, the Eastern Partnership need to address the above-noted challenges through both regional and country-specific actions. Good level of cooperation under the previous capacity building projects and mostly compatible legal background and practical experience across the region should be helpful in this respect.

10.1.4 Public/private cooperation and regional approach

Given the transnational nature of cybercrime and electronic evidence, effective international cooperation is essential. This includes police-to-police as well as judicial cooperation (mutual legal assistance). Key stakeholders include competent authorities within the Ministries of Justice, prosecution services and Ministries of Interior or police.

In recent years, the question of public/private cooperation and specifically the issue of criminal justice access to data has become more complex. This is also true for countries participating in the Eastern Partnership project. Often, local and multinational service providers are reluctant to cooperate, criminal justice measures and national security measures are not clearly separated, and trust towards authorities can be limited. Moreover, law enforcement powers such as those foreseen in the Budapest Convention on Cybercrime are not always clearly defined in criminal procedure law, and this adversely affects cooperation, erodes safeguards and implicates human rights and the rule of law.

The ultimate goal of public-private partnerships on cybercrime and electronic evidence is to ensure effective access by the law enforcement to data held by private entities - mostly Internet service providers – in the context of criminal investigations. Such access, which more often than not requires some degree of intrusion into privacy of individuals, requires clear legal basis to do so. Facilitating adoption of clear legislation based on the Budapest Convention and engaging local service providers in the process of discussions regarding development of law is a trust-building exercise, with trust being a key element in successful public-private partnerships. To this end, besides the Cybercrime Convention, standards and principles set by the 2008 Council of Europe Guidelines for cooperation between law enforcement and Internet service providers, as well as ongoing work of the Council of Europe, through T-CY and Cloud Evidence Working Group, to secure and further explore direct cooperation opportunities with the global/multinational service providers, is relevant to make such partnerships work.

Despite certain progress in this area, the eastern partnership region still faces the following challenges:

- Law enforcement powers such as those foreseen in the Budapest Convention on Cybercrime are not always clearly defined in criminal procedure law, and this adversely affects law enforcement/service provider cooperation as well as human rights and the rule of law. In at least two EAP states, public-private cooperation in cybercrime and electronic evidence has been hampered, chiefly among other reasons, by the absence of coherent legal framework for exercise of procedural powers available under the Budapest Convention on Cybercrime, as well as uneven practice of application of already available investigative powers.

- The issue of safeguards and guarantees is an important practical factor in terms of public-private cooperation. Availability, consistency and proportional use of specialized procedural powers by the law enforcement, beyond reasons of efficiency for investigations, contribute to clarity and foreseeability of law as well as protection from arbitrary interference with privacy of individual users and legitimate business of service providers.

- Cooperation agreements between the law enforcement and the Internet industry are believed to be the way forward to determine and regulate administrative and operational issues of public-private cooperation; at the same time, the existing arrangements in the region are either too narrow in scope, or not developed further, thus having a diminishing impact on maintaining trust between the parties. There is therefore need for more focus on more comprehensive cooperation agreements with more partners and

topics covered, taking into account the underutilized harmonization potential of the 2008 Council of Europe Guidelines for cooperation between law enforcement and Internet service providers.

- Despite the differences in the approach of Eastern Partnership states, one particular topic is of universal concern for the region: criminal justice authorities' access to data held by global/foreign communication service providers. As more data is being sought from such providers, cooperation is considered more challenging, compared to accessing data from private vendors/service providers established within national jurisdictions.

Although issues of public-private cooperation are primarily relevant in national contexts, the regional dimension of the problem is an important factor. Bringing the EaP countries together not only allows them to discuss challenges and issues, but also to learn from each other in terms of regulatory or institutional reforms. Peer-to-peer exchange of experience in the complex topic of public-private cooperation is important, as real-life examples of problem-solving by direct counterparts are appreciated more compared to more remote - often excellent - but still rather less relevant experience on the subject.

10.2 Recommendations

10.2.1 Refine approaches to cybersecurity

It is recommended that the Armenia, Azerbaijan, 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 cyber strategy elaboration should define and accept the basic terms (cybersecurity and cybercrime);
- A coordination committee should be convened prior to elaboration of a cyber strategy, to coordinate all stakeholders, monitor their compliance with their statutory remit and 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;
- Cyber strategy operations should be developed gradually among entities and/or people who have a trusted relationship;

- Cyber strategies should be open to insights from third parties with different knowledge and expertise;
- Cyber strategies 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 quantitative 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 cybercrime 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);
- Appropriate 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[40].

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[41]. 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 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. 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.

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

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

No specialized reporting mechanisms seems to be in place in all of the EaP states, which is often overlooked but is essential due to both nature of the crime in question as well as the state of technology and development right now, allowing for much simpler and wider solutions to be developed and deployed. 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).

Without detailed action plans listing the necessary responsible actors and resources for implementation, the cybercrime or cybersecurity strategies remain the statements of intent at best, which is an unfortunately frequent occurrence in the Eastern Partnership.

10.2.5 Develop international cooperation

Azerbaijan, Belarus, Georgia and Ukraine identify international cooperation as a priority. 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 or attend events that help to build capacity. This not only applies to technical expertise but also to the policy area.

Due to the cross border 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 cyber defence. 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[42]. 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

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

A multi-stakeholder approach is an essential element of cybersecurity strategies. 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[43] set up to define the cyber-approach and related national priorities. Another model is the Romanian Operational Council for Cybersecurity, headed by the Presidential Counsellor for National Security as Chairman and the Prime Minister's Counsellor 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 cyber strategies

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 authorities 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.

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 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 cyber strategy, 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

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).

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

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.[44] In addition, an academic research agenda derived from the cyber-strategy should be built to support government activities in this area.

---

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