Cybercrime@EAP 2018
International cooperation
Public/private cooperation

Արևելյան Գործընկերություն
Східне партнерство Eastern
Partnership აღმოსავლეთ
პარტნიორობა Parteneriatul Estic
Şərq tərəfdaşlığı Partenariat
Oriental Усходняе Партнёрства

Bucharest, January 2019

Perception of threats and challenges of cybercrime in the Eastern Partnership

Results of threat mapping exercise sessions in Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine 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

1 Introduction

Information about common cybercrime threats and challenges usually comes numerous sources, both nationally and internationally. However, without proper analysis and placement in the overall security context, such data has limited use or purpose. Therefore, analysis and sharing of information about threats and challenges of cyberspace between policy makers and professional communities should lead to better coordination and common approaches between all involved partners – both from state and private sectors. Ultimately, this should contribute to what should be the ultimate common goal: ensuring safer cyberspace for all.

Cyber threats could be defined as "the possibility of a malicious attempt to damage or disrupt a computer network or system". Analysing threats and challenges can be considered as one of the prerequisites of effective cybersecurity or cybercrime strategy. This enables countries to have a realistic and effective strategy document that would envisage the goals and actions that correspond to the needs of the country.

Having necessary information enables both policy makers and legislators to plan further actions including the finances, staff and measures and tools needed. Limited resources always mean that list of priorities should be established, and the most urgent problems and challenges must be addressed first. If country does the national risk assessment, then it should be also updated periodically in order to analyse situation in the past, and make predictions and plans for the future.

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 in winter/spring 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.

The national workshops on cybercrime strategies and threat assessment were held on the following dates:

6-8 February 2018 – Yerevan, Armenia
13-15 February 2018 – Baku, Azerbaijan
20-22 February 2018 – Tbilisi, Georgia
28 February – 2 March 2018 – Chisinau, Moldova
11-13 April 2018 – Kyiv, Ukraine
22-24 May 2018 – Minsk, Belarus

The current study is thus an attempt to summarize the discussions regarding threats and challenges of cybercrime during the above-noted workshops, and to present a brief overview of identified perception of threats, threat actors and possible responses to these threats by different national stakeholders.

2 Country summaries

2.1 Armenia

2.1.1 Threat mapping

In terms of major threats reported by the public sector, there is a division maintained between crimes against individuals, crime against business and security breaches affecting public agencies. The response to corresponding threats could thus trigger different responses.

In terms of top threats, personal data breaches (for example, attacks on personal social media accounts) and use of malware (in particular ransomware) are frequently noted. Attacks on financial sector and banking raise serious concerns, especially theft of personal and financial data (illegal access to accounts and personal data, theft of bank credentials, etc.). Phishing is also mentioned frequently as a persistent type of threat for Armenia, especially the one using social networks. Illegal access to information retained by ISP was one specific example mentioned in the context of Armenia.

There are also several types of threats that are defined by overall state security concerns. Crimes against state: systems, such as attempts to access critical information systems and hacker attacks on public and private enterprises, attacks against and defacement of public websites.

There are also specific threats for normal business operations. Along spam, attacks targeting large bookmakers/online gambling, interference into normal business between individual Armenian and foreigners (false invoices, fake/fraudulent emails used for "man in the middle" attacks business, interference with normal functioning and disruption with foreign counterparts' systems, interception of emails, etc.) is very specifically singled out as a major threat. DDoS attacks and frauds involving shopping on foreign websites are noted, but to a lesser extent.

In terms of overall **challenges**, overall network security, transfer of data beyond the jurisdiction of Armenia and server protection for most important services are frequently noted. There is no governmental established CERT, which poses great challenges for coordination and response.

The level of general awareness of the population remains one of the biggest challenges. Armenian citizens use operating systems that are out dated, and use of illegal/non-licensed software poses further risks. People's interest in applying cyber security measure is low (almost 60% percent of users are not concerned about cyber security measures and procedures) and some of them do not follow even the minimum requirements and advice from the authorities transmitted through the awareness campaigns. Examples include no use of strong passwords, no security for digital content, and no preoccupation in where they locate the stored data.

With regard to **threat agents** and actors, the following table demonstrates the overall approach to threat agents in relation to specific threats:[1]

[1] "**P**" standing for primary actor and "**S**" – for secondary; blank space means "not relevant".

Cyber Threat	Threat Agents						
	Cyber criminals	Insiders	Nation states	Corporations	Hacktivists	Cyber fighters	Cyber Terrorists
Malware	P	S	P	P	S	S	S
Web based attacks	P		P	P	P	P	P
Web app attack	P		P	P	P	P	S
DDoS	P		S	S	P	P	S
Botnets	P		P	P	S	P	
Phishing	P	P	P	P	P	P	
Spam	S	P	S	S			
Physical manipulation damage	P	P	P	P	S		S
Exploit kits	P		P	P		S	
Data breaches	P	P	P	P	P	P	P
Identity theft	P	P	P	P	P	P	S
Ransomware	P	S	P	P		S	
Insider threat	P		S	P		S	S
Information leakage	P		P	P	S	S	S
Cyber espionage		S	P	P		S	

2.1.2 Main actors responsible for security of cyberspace

The **Ministry of Justice** has a main role in developing the legislative framework and also the organizational tasks within the government sector regarding codification and the legal reforms. The Ministry is also a forum to generate informal cooperation between the public and the private sectors. The Ministry of Economy and the Ministry of Transport are active peers to the Ministry of Justice within the government.

The **Prosecutor General's Office** has the responsibility to control and to supervise the investigative procedures. In practical terms, if any investigative measure is applied unlawfully by the investigating entity, the prosecutor can impose disciplinary actions against the investigator; to date, no ISP has challenged requests for information during an investigation.

The **High-Tech Crime Department of the National Police** is a centralized unit which is dedicated to handle cybercrimes with a country wide competency. Police has 10 days to determine the fundamental facts and the legal basis for the investigation itself and then deciding to either: close the matter; send case to local police where evidence or perpetrator is located; or transfer the matter to the Investigative Committee. Thus, the Department is the primary police unit handling cybercrime cases at the preliminary stage (before official investigation is opened by the Investigative Committee) and providing support to local units. The Police also have preventive responsibility and with cooperation with the media share some information for prevention purposes.

Investigative Committee handles 95% of the criminal cases in Armenia, the others investigated by specialized units for tax and customs fraud or investigations into public officials. The Committee has 3 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 dispose of a computer forensics laboratory but instead will make use of external expertise for the analysis of electronic evidence.

The **Data Protection Authority** (DPA) is quite new, since it was set up on 9 October 2015 based on the initiative of the Prime Minister. The Commissioner of the Authority is appointed for 5 years by the Ministry of Justice pursuant to a list of candidates established by 5 non-governmental organisations. The decision to choose the Commissioner is made with the support of the Prime Minister. The Commissioner can only be relieved of his position on predefined exceptional grounds. The DPA has a staff of 10 persons, including a technical expert for any needed forensics investigations, who is undergoing technical training.

The critical infrastructure and any other vital services are subject of the **National Security Service** protection. The Agency is also in charge with protection of sensitive information.

The **national CERT** - CERT.AM - is a part of the Internet Society of Armenia, being a non-governmental entity but already has a good and active working relationship with the police. One of the main tasks of the CERT is managing the root of the .AM top-level domain system, and to support the government in case of requests. The CERT regularly provides Internet Access Providers with information about problems on their networks such as amplification attacks.

The **state owned company E-KENG** provide e-governance services (ex: electronic appliance for visa, e-health) in Republic of Armenia. The company operate a platform for these services and also the most of the data base. If interference, leakage or irregular activities are noticed the company have to report it, stop the access to the system and notify to the DPA and the Police. Once the GD for data protection will be approved and its provision implemented sanctions are going to be applied for failure to comply.

There are over 100 **Internet Service providers** working in the country including five major landline internet access providers and three major mobile carriers. All ISPs in Armenia are private, which makes security of Armenian cyberspace dependent on efficient public-private partnership.

In terms of **information sharing** regarding threats and cybercrime, the law enforcement is of the general opinion that private sector is not very much willing to report any incidents to the police. Vice versa, there is also no practice of sharing information with the private sector for preventive purposes. The interagency reporting, through, is implemented between multiple stakeholders, including Central Bank, Prosecutor's Office, Investigative Committee and the National Police. Some sharing of information happens if law enforcement agencies need specific expert assistance for investigations from the private sector (frequent basis for this is MoU between ISPs and Investigative Committee).

2.1.3 Mitigation and response

Developing of the existing national CERT seems to be the most pressing need and option for Armenia. Also, setting up clear responsibility to this structure, allotting necessary resources, and establishing terms and conditions to fulfil, it would be more than necessary and useful. A CERT structure could be a very good feed to security services and law enforcement for identifying cyber threats that affect national cyber space, and be a good partner for the LEA by providing technical support.

Educational programmes need to be developed. For this purpose, organisations that possess the necessary knowledge will need to (re-)shape the corresponding skill profile and combine capabilities to develop comprehensive education curricula.

The development of better cyber-defences requires new combination of skills and knowledge. Policy needs to create proper conditions that will lead to better education in the area of cybersecurity and in particular in cyber threat intelligence.

The cybersecurity community needs to elaborate on technical solutions that will allow for lawful interventions in cyberspace that do not jeopardise privacy and security properties of user data (i.e. confidentiality, integrity and availability of information).

Some other considerations may be brought forward:

- Encourage drafting and implementation of national cyber security strategy;
- Consider feasibility to introduce data retention provisions into the electronic communications legislation;
- Conduct regular scenario cyber exercise that provides a picture of national cyber space;
- Develop a central registry for national level incidents;
- Promote cooperation with other national CERTs for threat intelligence sharing;
- Formalize coordination regarding to critical infrastructure protection;

- Elaborate a National risk assessment plan to better understand the specificity of the national cyber space and take proper measures to defend it.
- Build trust with the private sector and the industry
- Improving cooperation with Interpol and Europol for cyber crime cases
- Building trust and improving interagency cooperation and exchange information (security as a national goal)

The Armenian authorities are aware about the necessity of raising the cyber security level of the general population. Public awareness campaign is conducted by different stakeholders. As an example, the Data Protection Agency, during the last period, produced six guides with cyber security rules for the population.

2.2 Azerbaijan

Data removed at the request of authroties of Azerbaijan

2.3 Belarus

2.3.1 Threat mapping

The **threats** identified by the authorities of Belarus focus on common security threats and crime landscape. In this regard, use of malware and in particular ransomware is noted as the major threat; a specific case of crypto-mining malware (acting as sabotage tool) is noted as a threat in this regard as well. DDoS attacks still remain viable threats, especially ones with high level of sophistication. Data breaches (unauthorized access to accounts) are another area for concern. And in terms of security of state systems, cyber sabotage is regarded as a threat. Cybercrime as a service remains high on the list of threats for authorities of Belarus.

On threats directed against the private sector/business interests, phishing is considered as a major threat. Business email compromise and CEO fraud, as well as banking and credit card fraud are noted to be the most common threats in this regard. In similar fashion, abuse of credit card data and captured PINs is a more specific case of threat relevant for the stakeholders in Belarus. Threats related to use of key-loggers and legal SIM-boxing have notable relevance as well.

In terms of the threats identified by the Internet industry, unsurprisingly these refer to business models and operations of the sector. Phishing, business email compromise and ransomware are listed as top threats. Quite unusually, DOS/DDOS and brute force attack are still a concern. SMS spam continues to be a perceived problem. SQL injections, cross-site scripting and data leakage are listed as technical but still very relevant threats for the industry. Illegal VOIP abuse is another type of threat relevant for communications companies. Last but not least, malicious web advertisements are considered to be a threat, as well as vulnerabilities of specific accounting software used in the industry.

In terms of **challenges**, Belarus seems to favour strong law enforcement / criminal justice response to threats emanating from cyberspace; therefore, wide-ranging nature of threats from cyber-enabled crime and issues of access to electronic evidence in criminal cases remain top challenges for Belarus. Money laundering and crime proceeds related to cybercrime are also noted frequently as threats connected to cybercrime/cyber-enabled offences.

With regard to **threat agents** and actors, the following table demonstrates the overall approach to threat agents in relation to specific threats:[2]

[2] "**P**" standing for primary actor and "**S**" – for secondary; blank space means "not relevant".

Cyber Threat	Threat Agents						
	Cyber criminals	Insiders	Nation states	Corporations	Hacktivists	Cyber fighters	Cyber Terrorists
Phishing	P					S	S
Data Breaches (unauthorized access to accounts)	P	P					
Banking/Creditcard Fraud	P	P					
Malware (Global)	P	S	P			P	
Ransomware	P	S	P			P	
Cyber Sabotage		P					
Cybercrime as Service	P						
Cryptomining malware (as sabotage)	P	P				S	S
DDoS	P			P	S	P	P
Abuse of Credit Card data/captured pins	P						
Keyloggers	P	P	S				
Business Email Compromise/CEO Fraud	P						
Cyber Enabled Crime / Electronic Evidence							
Illegal Simboxing	P						
Money Laundering/Cybercrime related	P			P		S	S

2.3.2 Main actors responsible for security of cyberspace

The **Ministry of Justice** has a main role in overseeing the legislative framework and also the organizational tasks regarding codification and the legal reforms. The Ministry also supervises the expert board which has a key role in evidence and forensic work.

The **Prosecutor General's Office** has the responsibility to control the investigative procedures and at the same time the prosecutor's may issue requests to the ISPs in order to provide them subscriber and traffic information. Prosecutor's Office also has the primary responsibility for international cooperation on cybercrime and production of statistics on crime. Mutual legal assistance procedures are implemented and are applied by the Office.

The **Ministry of Internal Affairs** has a dedicated High Tech Crimes Department. The Department has 30 officers specialised in cybercrimes and 3 specialists as well in each of the country's 6 counties. 70% of MIA cases concern fraudulent withdrawals of money from ATM machines through forged credit cards which are prosecuted as theft. The remaining cases mostly concern unauthorized access into computer systems through hacking and other types of information security crimes. The Ministry of Internal Affairs manages the pre-investigation phase for 99% of the cases. The pre-investigation phase can last for a maximum of 3 months before the case is passed on to investigation with the investigative committee.

Since 2012 the **Investigative Committee** is an official independent investigative authority of the Government. The Investigative Committee investigates about 99% of all crimes, including cybercrime. The Investigative Committee has a website where citizens can report cybercrime. Although the Investigative Committee sets out which information should be sought, the search orders are generally carried out by the Ministry of Internal Affairs.

The **Ministry of Communications and Informatisation** is the national regulator in charge of developing the relevant legislation. It is their responsibility to put the legislation into practice. It

was reported that Ministry's main aim is to develop the regulatory framework with continuous communication with the private sector. The Ministry set up the State program on Informatisation and on "Electronic Belarus" which both played key roles in the cyber domain. Transferring data over the Internet is a regulated activity that is allowed by a license under the supervision of the Ministry. The Department of Informatisation within the Ministry is currently dedicated to supervise data protection issues.

The **Inspection on Communication** is a government entity is analysing and gathering the illegal information on the Internet. The Inspection manages and supervises the access of all ISPs in the country (~150) and continuously keeps a list of hackers active in relation to the country.

The **Operational and Analytical Centre** is an institution founded by the President and remains under presidential reporting as well and has mandatory powers to act in its field. The Centre's main role is to organize the cooperation related to ICT within the government sphere and its key focus areas are internet security, the support and supervision of critical infrastructure (both public and private), and the regulation on cryptography. They have cooperation on an international level as well if an attack has a cross border effect, but this is only in reactive mode and not regular. The government cloud project (G-Cloud) is managed in the BeCloud framework.

The **national CERT** under the OAC manages and handles the cyber security threats and incidents which may occur in relation to the public and the private sector users as well. The activity is set up the way that they don't only focus on reactive measures, but also on proactive approaches. The entity has a staff of 12 professionals on board. They are entitled to develop their own by-laws.

There are about 150 **Internet Service providers** working in the country. It shall be noted that before 2010, servers were generally outside of the country's borders. Based on Presidential Order Nr. 60 ISPs are currently not allowed to provide any services from outside of the country. Now all of the hosting is under the supervision of Beltelekom and all providers are in the system of the United Data Transit Network.

2.3.3 Mitigation and response

There are common threats and challenges identified by both state agencies and private sector; although, as may be expected, the authorities' list includes a range of crime-related issues, and the industry list is more focused on security. The common threats are a clear indication of the need for collaborative action to meet these threats.

Development of an all-encompassing cybersecurity and cybercrime strategy would enable Belarus to further build capacity to meet the challenges posed by these threats and have a benchmark to measure future progress.

The lack of legislation covering the possession of child abuse materials is concerning and should be addressed, to ensure that this type of behaviour is suitably criminalised.

Training for judges both at introductory and in-service levels should be considered.

Investigators are willing to inform stakeholders in individual cases. Shortfalls in institutions can be communicated to regulators and other supervisory authorities. This is a very effective measure in practice and should be maintained.

Mass media is currently used to address topical threats and this practice should continue as well.

2.4 Georgia

2.4.1 Threat mapping

Georgia has both dedicated Cybersecurity Strategy (valid until end of 2018) as well as cybercrime strategy as a part of the Organized Crime Strategy. Because major threats are identified in these

strategies as result of national threat review, the discussions with Georgian stakeholders were not focused on developing threat mapping, as the threats noted specifically in Cybersecurity Strategy are believed to be of common understanding:

Cyber war – since 2008, remains an ongoing concern due to proliferation of cyber weapons and techniques in cyberspace, as exemplified by recent cyber operations ongoing against Ukraine;

Cyberterrorism - the threats related to cyber terrorism and scale of anticipated damage have escalated, as terrorist groups acquired significant resources and knowledge of information and communication technologies, which are actively used with the purpose of supporting their activities, including use of social networks for recruitment. In addition to the cyber-terrorist threats stemming from the terrorist organizations, the targeted cyberattacks organized by the State actors are also perceived to be important, as the latter possess and permanently develop significant cyberattack capabilities;

Cyber intelligence activities – cyber intelligence is mainly carried out by the organized powers with the objective to obtain sensitive information containing state secret, as well as other type of closed information. Cyber espionage software means are perceived as malware types specifically contributing to this threat;

Other activities directed against Georgia using cyberspace - one of the challenges for the Georgian security are crimes committed with the use of cyberspace, which are directed against the private and public infrastructure providing critical services to Georgia. During the recent period, attacks against the suppliers of financial and communication services have become more and more dangerous with the consideration of the fact that all subjects critically significant for Georgia depend on these services. Accordingly, breakdown of functioning of financial and communication sectors also conditions paralyzing of normal operation of other critically important subjects.

The discussion with Georgian counterparts also outlined the main cybercrime and cyber-related threats that affect Georgia from their perspective. Most of these threats are related to banking and financial sector. Also government information systems that are used to process state secrets and personal data are considered to be at risk. Critical infrastructure protection and protection measures were highlighted and the need for information security standards. Malware, ransomware and other APT related threats were mentioned as well. The telecommunication sector has had problems with frauds related to the use of SIM-boxes.

The following list could be used to summarize the identification of major threats and challenges related to cybercrime:

Threat Types

Phishing
Malware
Spear Phishing/Pharming
IPv4 v6 migration
IOT security

Threat Sources

Organised Crime Groups
Terrorists (increasingly prevalent)

Targets

State agencies
Private Sector Organisations
Personal Data
Banking Sector
End Users

Private sector and society are generally considered to be more vulnerable to cybercrime and cybersecurity incidents. At the same time, rather surprisingly, specific threats of malware and ransomware are not reported to be problematic for the industry.

2.4.2 Main actors responsible for security of cyberspace

The **Ministry of Justice** has a main role in developing the legislative framework and also the organizational tasks within the government sector regarding codification and the legal reforms. The Ministry is also a forum to catalyse cooperation between the public and the private sectors; it also had a role in developing the Memorandum of Understanding between the law enforcement authorities and the ISPs in 2009 and 2010.

The **Prosecutor General's Office** has the responsibility to control and to supervise the investigative procedures. Cybercrime related investigations are based on the Criminal Procedural Code, meaning no specific regulation was introduced in this respect. Prosecutors must show probable cause in case of search and seizure. There is only one prosecutor on staff who is especially focused on cybercrime issues.

The **Ministry of Internal Affairs** has a dedicated Cybercrime Unit within the Criminal Police Department. The Cybercrime Unit was founded in 2012 and currently has 15 officers on their staff and their technical support is provided by in-house professionals.

The **State Security Service** has the following main units regarding cybercrimes: crisis management, digital expertise and technology, furthermore, international relations. The Service has an active role – together with the Crisis Management and Security Council - in developing the new Cyber Security Strategy which shall be approved in this year and shall be effective until the end of 2018.

The **Georgian National Communications Commission** (GNCC) is an independent public administration body, which reports to the parliament on an annual basis. Its annual report is published on its website. With a staff of 120 people, its mandate is to regulate electronic communications and broadcasting sectors of Georgia.

The **Data Exchange Agency** was established in 2010 as an independent body. Its main aim is to coordinate e-governance and strategy, furthermore international projects and cyber security. It has a significant effect on development, legislation, international relations and raising awareness. The implementation of the ISO 27xxx family is a key project of the Agency. The Agency has established an incident management system which enables them coordinate and exchange information with critical infrastructure entities. For the critical infrastructure entities, consultation and assistance has been provided in order to implement the ISO standards.

The **CERT.GOV.GE** under the Data Exchange Agency is one of two dedicated governmental CSIRTs in Georgia: the CERT.GOV.GE and the Ministry of Defence CERT. The Law on Information Security defined that the government CERT is responsible for the handling of incidents, providing alerts, raising awareness and educating (e.g. penetration testing). The protection of the Georgian critical infrastructure is a priority task; there is no national CERT operating currently in Georgia, although the CERT.GOV.GE is currently performing these functions.

The **Office of the Personal Data Protection Inspector** is an independent body with an annual reporting obligation to the parliament. The Inspector in charge of the authority is appointed by the Parliament. The main tasks of the Office are: consulting, handling of citizen complaints, inspections / audits, awareness raising and setting up standards / education, providing recommendations and international relations in the topic. From 2019, it will also have fully independent investigative powers.

There are around 110 **Internet service providers** in the Georgia, 32 having their own IP addresses, and the others being virtual operators. Silknet and Causasus Online are the two largest providers with around 80% market share together. In early 2016, the Small and Medium Telecommunication Operator's Association was established, for the purpose of bringing together

the small ISPs, but also cable TV operators, transit and telecom operators. As of May 2016, the association has 35 members.

2.4.3 Mitigation and response

Georgia is fairly advanced when it comes to cyber security and uniform perception of threats and challenges, as evidenced by recent international and European rankings.

As the current set of cybersecurity and cybercrime strategies draw near the end of their respective cycles, development of a cybercrime strategy as a component of the national cybersecurity strategy and on the basis of up-to-date perception of cybercrime threats and challenges would be beneficial.

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 was reported as effective by both public and private sector stakeholders, although the private sector was more of an opinion that the documents works to far lesser degree than few years ago; since it is one of the greatest opportunities to ensure security of cyberspace through cooperation, the Memorandum could be updated.

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. This practice is highly beneficial and should continue.

2.5 Moldova

2.5.1 Threat mapping

Both public and private sector are fully aware of the threats and risks originating from cyberspace. While private sector entities and NGO-s are more worried about cybercrime, government sector, law enforcement, intelligence services and military are concerned more about rising number of cyber incidents and cyber-attacks. When talking about cybercrime then most often it includes ransomware, online fraud, attacks against networks and critical infrastructure, offences related to cryptocurrencies, offences related to manipulation of data and illegal access. Other offences include hate speech and social media abuse, online radicalisation, grooming and distribution of child abuse materials, espionage and money laundering.

Most of the threats are considered originating from ordinary criminals. There is also sufficient information to believe that behind certain activities are also hacktivists and cyber fighters, terrorists as well as nation states. Ransomware distribution, attacks against computers and networks, including attacks against critical infrastructure are being often committed by hacktivists, fighters and terrorists. Large-scale cyber-attacks are supposedly often committed by nation states, although it is difficult to obtain electronic evidence enabling attribution.

Often cyber incidents and cybercrime occur because of low awareness of cyber threats, lack of training and education and non-implementation of basic information security principles and policies. Although public and private sector together have taken steps to raise awareness about information security and cyber hygiene, still often incidents occur due to lack of proper information security policies and standards, insider activity, use of illegal or compromised software and human errors. Often cyber incidents have resulted in data breaches, theft of data, encryption or destruction of data and related extortion.

Private sector entities have suffered a lot from ransomware, and computer related fraud (online payment fraud, business e-mail compromise or CEO-fraud). Entities involved in audiovisual media

have concerns with fake news and manipulating with the public as well as hate speech and illegal content online.

With regard to **threat agents** and actors, the following table demonstrates the overall approach to threat agents in relation to specific threats:[3]

Cyber Threat	**Threat Agents**						
	Cyber criminals	Insiders	Nation states	Corporations	Hacktivists	Cyber fighters	Cyber Terrorists
Ransomware	P	S	P			S	S
Cyberattacks (frozen conflict)	S		P			S	
CAM and hosting in Transdnistria	P						
Cryptocurrency fraud/embezzlement	P	S	S				
Illegal crypto mining	P	S	S				
Social media abuse/Blue Whale	P		S		S	S	P
Hate Speech/Incitement	P		P		S	P	P
Critical Infrastructure Attacks	P	P	P	S		P	P
Radicalization via Social Media	S		P			P	P
Online Payment fraud (also mPay)	P	S	S			P	S
Botnets	P		P			P	P
Grooming	P						
Information security vulnerabilities	P	P	P	P	P	S	P
Pirated and Trojanized Software	S						
CEO Fraud/BEC fraud	P	S		S			
Money Laundering with Cryptocurrency	S			P			
Data Breaches and Extortion	P	P	S	P		S	S
Counterfeiting and Smuggling/forgery of data	P			P			
APT (State sponsored)	P	S	P	P			
Fake news and manipulation	S		P	P		P	S
POS Fraud	P						
Insider Threats		P	S	S			
Industrial Espionage			P	P		S	
Malware	P		P	S	S	S	P
ClickFraud and Phone Fraud/Flooding				P			

2.5.2 Main actors responsible for security of cyberspace

The **Ministry of Justice** has a main role in overseeing the legislative framework and also the organizational tasks regarding codification and the legal reforms.

[3] "**P**" standing for primary actor and "**S**" – for secondary; blank space means "not relevant".

The **Prosecutor General's Office** has the responsibility to control the investigative procedures and at the same time it may issue warrants as well with a limited scope. 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 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. The Prosecutor General's Office is responsible for the oversight and control of interception. This task is managed by a separate unit within the office, which prepares a report twice a year to the Parliament and the President.

The **Ministry of Internal Affairs** has a dedicated The Centre for Combating Cybercrime within the General Inspectorate of Police has an active communication bridge with Facebook, Skype (Microsoft), Western Union, Webmoney, Paypal and eBay. The Centre plays an important role in providing their opinion to the Parliament as well on how to reform the relevant laws to battle cybercrimes (e.g. extension regarding the preservation of data). They have a good international cooperation with their professional peers (e.g. with Italy, Estonia, international expert bodies, etc.). A reporting mechanism for citizens and legal entities to report internet crimes is being considered but an implementation project has not yet been decided. It is however possible to report crimes by email.

The **Security and Intelligence Service** has a supporting role in collecting and analysing data related to cybercrime, thus it is not proceeding as an investigative body (they don't perform interrogations, but they may interview persons). The investigations which are supported by the Service are generally undertaken by the Ministry of Interior and the General Prosecutor's Office. They have an active cooperation with their local peers and also on an international level in order to handle cyber threats.

There is only one operational CSIRT in the Republic of Moldova – "**Cyber Security Centre CERT-GOV-MD**". It was established in 2010 by Government Decision No. 746 of 2010 "On the approval of the updated Individual Partnership Action Plan the Republic of Moldova - NATO". The team took responsibility for handling of information security incidents and offering other cybersecurity services to public administration authorities of the Republic of Moldova. However, due to the lack of national CSIRT and wide national and international cooperation capacities of Cyber Security Centre CERT-GOV-MD the centre became the main point of contact for cybersecurity incidents related to the Republic of Moldova. There are five experts working in CERT-GOV-MD. The CERT-GOV-MD cooperates with law enforcement agency – Centre for Combating Cyber Crimes in the following areas: fighting with cybercrime (by reporting suspected incidents), capacity building (by organizing joint cybersecurity workshops and trainings), awareness raising (by organisation of cyber security conferences). Cooperation with state institutions is mainly based on internal regulation, bilateral agreements and voluntary commitments.

The **National Centre for Personal Data Protection of the Republic of Moldova** was founded in 2009 and it has a new director since April 2016, who was elected by the Parliament. The Centre generally has the right to provide its data protection focused comments to the codification bodies.

The **Internet service providers** consider themselves to not be liable under the current legislation either to preserve or to retain the data. In general, the private sector in Moldova is rather hesitant to work with law enforcement than what is normally expected in the country context.

As regards cybersecurity incidents, ISP-s need to report to national CERT, if incident is serious. As Cybercrime Centre has also MoU with CERT-MD, it is possible to start a criminal investigation if necessary.

2.5.3 Mitigation and response

Since 2015, in Moldova there is a separate section No. 4 entitled "Preventing and combating cybercrime" in the National Programme on Cybersecurity 2016-2020. Other sections of the

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. 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. However, these provisions still need to manifest themselves into coherent, officially adopted and endorsed cybercrime and cybersecurity strategy, with specific and viable action plan to implement its provisions.

The public-private cooperation needs serious improvement, as this could be the most crucial block in ensuring security of cyberspace.

There are no specific prevention programs on cybercrime. Still, in 2017, Safe Online campaign was organised in schools which included awareness raising, lectures and distributing information booklets and flyers. There have been also advertisements on media as well as warnings and guidelines on how to recognise or identify victims of online violence.

Special attention is paid to children and protecting children online. There is an Action Plan on Protecting Children Online. Cooperation with private sector and NGOs is deemed crucial in this respect. For example, there has been cooperation with La Strada to raise awareness and share information as well as cooperation with ISP-s, specifically on the issues of child abuse online.

2.6 Ukraine

2.6.1 Threat mapping

Firstly, it should be mentioned that public awareness about the cyber-related risks has increased a lot during last years. One of the main reasons for this is massive malware campaign against Ukrainian public and private networks and computers as well as cyber espionage and and cyber attacks against public that have taken place during recent years.

As a result of these incidents whether both public and private sector entities suffered, including economic losses, more and more attention has been paid to information security, cybersecurity and prevention of cybercrime.

The main threats include cybercrime offences such as fraud, illegal access to computer systems and networks, DDoS attacks, different malware, ransomware and wipe attacks. Often attackers are aiming at confidential information and personal information of government officials. Therefore cyber espionage has occurred often. When there has been data breach or theft of data, including from government databases, sometimes data has been offered for sale by the criminals.

Ukrainian authorities have witnessed advanced persistent threats and coordination and planning of the attacks. There have been cases of cooperation between the perpetrators and insiders. Often phishing and social engineering attacks have taken place earlier in order to obtain credentials or other information that can be used to launch an attack against the computer system or network. Attacks against computer systems and networks have several times included attacks against critical infrastructure. Law enforcement and intelligence see also crime as a service pattern emerged. In order harm or paralyse computer systems and network, including those belonging to the government or critical infrastructure, physical attacks against network infrastructure, including copper and fibre optic cables have occurred.

Although most of the cybercrime is committed by the criminals, there is still reason to believe that often hacktivists, cyber fighters and terrorists can be behind the attacks. Large-scale attacks that are complicated and require lots of resources and efforts to prepare, could have been state sponsored. On different social media sites and foreign media outlets information operations and fake news campaigns have been detected with a primary purpose to cause distress and confusion among the population as well as create a negative image of government and the country.

With regard to threat agents and actors, the following table demonstrates the overall approach to threat agents in relation to specific threats from the Governmental sector:[4]

Cyber Threats	**Threat Agents**						
	Cyber criminals	Insiders	Nation states	Corporations	Hacktivists	Cyber fighters	Cyber Terrorists
Cyber fraud/banking/payment fraud	P	P	S	P			
Illegal access to computer systems and data	P		P	P	P		
DDoS attacks	P		P		P	S	
Malware attacks	P	P	P	P			
Data breaches/leaks		P		P			
Wipe attacks	P		P				
Ransomware	P		P				
Social engineering attacks/phishing	P	P	P	P			P
APT	P	P	P				
Stolen credentials/illegal access							
Intellectual property offences	P			P	P	P	
Cyber attacks against Government databases	P		P				
Insider atacks	P		P				
Sale of personal information	P	P	P	P	P	P	P
Crime as a service	P		P	P	S		
Cyber espionage	P		P	P			
Informaiton operations / fake news			P	P	P		

However, there is also a different – and far more detailed - perception of threats and challenges from the private sector entities (mostly Internet service providers):

[4] "**P**" standing for primary actor and "**S**" – for secondary; blank space means "not relevant".

Cyber Threat	Threat Agents						
	Cyber criminals	Insiders	Nation states	Corporations	Hacktivists	Cyber fighters	Cyber Terrorists
DDoS	P		S	S	S	P	P
Identity theft/Phishing	P		P	P	S	S	S
Banking malware/Trojans	P	S	S			S	S
Botnets	P		S	S	P	P	P
Copper theft		S	P			P	P
Sabotage of fiber-optic cabling		S	P			P	P
Espionage on topology and cable maps		S	P	S		P	P
VoIP Attacks (PBX hacking using premium numbers)	P	P					
Social media account takeover	P				P	P	P
Falsified websites (of known banks) - social engineering	P						
Business email compromise	P						
False websites, ID theft	P				P	P	P
Abuse of default password of IoT devices	P	S	P	P	P	P	P
Copyright violations	P						
Abuse of trademarks (squatting, counterfeit)	P			P			
Torrent trackers	P						
Torrent index sites	P						
Retracker services	P						
DDoS and extortion	P		S		P	P	P
SS7 attacks	P		P				
Interception of geolocation	P		P				
Interception and rerouting sms messages	P		P				
Interception of comms made possible	P		P				
State sponsored attack on infrastructure.			P		P	P	P
Attacks on power grid	S		P		P	P	P
Installation of malicious software on control systems	S		P		P	P	P
Malicious software used against Ukraininan systems	S		P		P	P	P
Creditcard fraud	P	P					
Skimming	P						
Card not present	P	S					
Ransomware	P		S				
Romance fraud	P						
Tech support	P						
Advance fee fraud	P						
BGP Attacks	P	S	P	P	P	P	P
Infrastructure no longer under de facto control		P	P				

2.6.2 Main actors responsible for security of cyberspace

The **Ministry of Justice** has the main role in developing the legislative framework and also the organizational tasks within the government sector regarding codification and the legal reforms. Currently a legal reform is being discussed regarding a more detailed content focused cybercrime initiative for the criminal legislation

The **Prosecutor General's Office** has the responsibility to control and to supervise the investigative procedures. There are plans to introduce specialized prosecutors who would be trained and have necessary experience in cybercrime investigations.

The **National Police** has a dedicated Cyber Police Department. Since its foundation in 2009, the Cyber Police only acts as a specialist force that is supporting investigations from the technological point of view, meaning that they are not performing any core investigations – there are undertaken by investigators based on investigative jurisdiction. The total number of their staff is 39. There are dedicated units within police in the following subjects: e-commerce, online gambling, IPR / pharmacy, financial frauds, credit cards, skimming, online banking intrusions, e-currency frauds and child pornography.

The **State Security Service** provides main focus to secure national security and to protect the country's cyber sphere, focusing on counteraction to cyberterrorism, protecting state informational resources and critical infrastructure from cyberattacks, fighting with transnational cybercrime, which are the major issues. The recent Law of Ukraine on Basic Principles of Cyber Security further developed the mandate of the service in terms of cybercrime investigations, and provided more clarity in terms of division of powers to investigate vs. the Police: 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.

The **National Commission for the State Regulation of Communications and Informatisation** (NCCIR) was established in 2011 and its procedures are based on the Law of Ukraine "On Telecommunications". It is responsible *inter alia* for the licensing, regulation and supervision of the telecom, postal services and ICT sectors. The NCCIR reported around 5000 ISPs in the country. In case of breaching of the relevant regulations an ISP's managing director can be fined. The NCCIR admittedly plays a very modest role in regulating ISPs, specifically regarding ISPs' cooperation with the law enforcement.

The governmental **CERT** within the Special Communications Service provides incident investigation, consultancy (including penetration testing) and monitoring. It is one of their main tasks to support implementation of ISO standards (27xxx). The staff may also proceed as a team of experts at court. It was reported that the cooperation with local ISPs is low. Draft legislation is being debated about setting up further and sector focused CERTs in the country. The CERT has a significant role in drafting the cyber security strategy.

According to the amendments to the Law of Ukraine «On Protection of Personal Data» introduced in 2014 the function of control over observance of the legislation on protection of personal data is assigned to the **Ukrainian Parliament Commissioner for Human Rights:** the Ombudsman's Office.

Regarding **Internet service providers,** there are about 5,000 business entities in the registry of operators of telecommunications (including ISPs) in Ukraine. According to official information from the web site of Ukrainian Internet Association, it consists of 129 active members and 61 associated members, representing mostly large and active entities out of those. The Association is very active on the topics of cooperation with the law enforcement.

2.6.3 Mitigation and response

The current Cyber Security Strategy is implemented through yearly action plans. Although there is nothing inherently wrong with this approach, consistent funding for implementation of these action plans remains a challenge and should be a priority task to address.

Police reported that the cooperation with the major ISPs needs development on the part of the business, and there is still lack of trust in general (although situation is improving). There is currently 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.

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 formal Memorandum of Understanding 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 adoption of this document should boost cooperation for the security of cyberspace.

There is an obligation for critical infrastructure objects, identified in the recently adopted Law of Ukraine on basic principles of providing cyber security in Ukraine, to report cyber incidents. However, technical and practical details for efficient cybercrime reporting still need to be developed.

3 Conslusions

As many other states across the globe, 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 countries, which can be grouped into three main categories:

- Conventional cybercrime: 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[5] rather than a specific uniform feature of the Eastern Partnership, and thus should not be taken as such. Another objective reason for this could be the prevalence of state actors for the majority of EaP states when it comes to major sources of cyber threats, as almost all of these states are involved in rather complex and challenging relations with their immediate neighbours.

The EAP region retains its potential as a platform to carry out cybercrime activities with targets elsewhere; the recent examples of ransomware attacks and cyber-attacks on power grids/critical infrastructure 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.[6]

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

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

[6] See iOCTA report (2014), especially pp. 21 and 28.

security standards, i.e. finance and banking, governments can establish additional standards to enhance protection.

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.

At the same time, there is a lack of strategic approaches to countering cybercrime and making use of electronic evidence in criminal proceedings, as reflected in the absence of dedicated policy documents on cybercrime and electronic evidence as mainstream challenges of criminal justice systems. Even where cybercrime-related provisions are found in strategies or action plans, they are placed within an overall framework of organized crime strategies or cyber security documents. This hardly addresses the problem of cybercrime as a major criminal justice challenge.

Even where strategies exist, the development of these documents hardly proceeds on the basis of clearly identified, measurable and commonly agreed understanding of threats and challenges that are shaping the security of cyberspace in individual countries. There was not a single jurisdiction of the Eastern Partnership that has shown any meaningful involvement of the private sector in the process of development of such strategic visions and documents. This runs against a fairly common understanding that the majority of critical information systems that such strategies and action plans need to address are owned and run by private business entities, who also become stakeholders in the process of ensuring security of cyberspace.

In consequence, criminal justice systems lack resources and capacities to prevent, investigate, prosecute and adjudicate not only cybercrime but the growing number of other offences involving electronic evidence. Clearer policies, more specific plans and allocation of resources for the criminal justice response to cybercrime and electronic evidence are needed. Therefore, in the future, this particular exercise could benefit from repletion with more details, and with more objective sources of data, to define and inform the response from the Eastern Partnership states to security challenges of cyberspace.