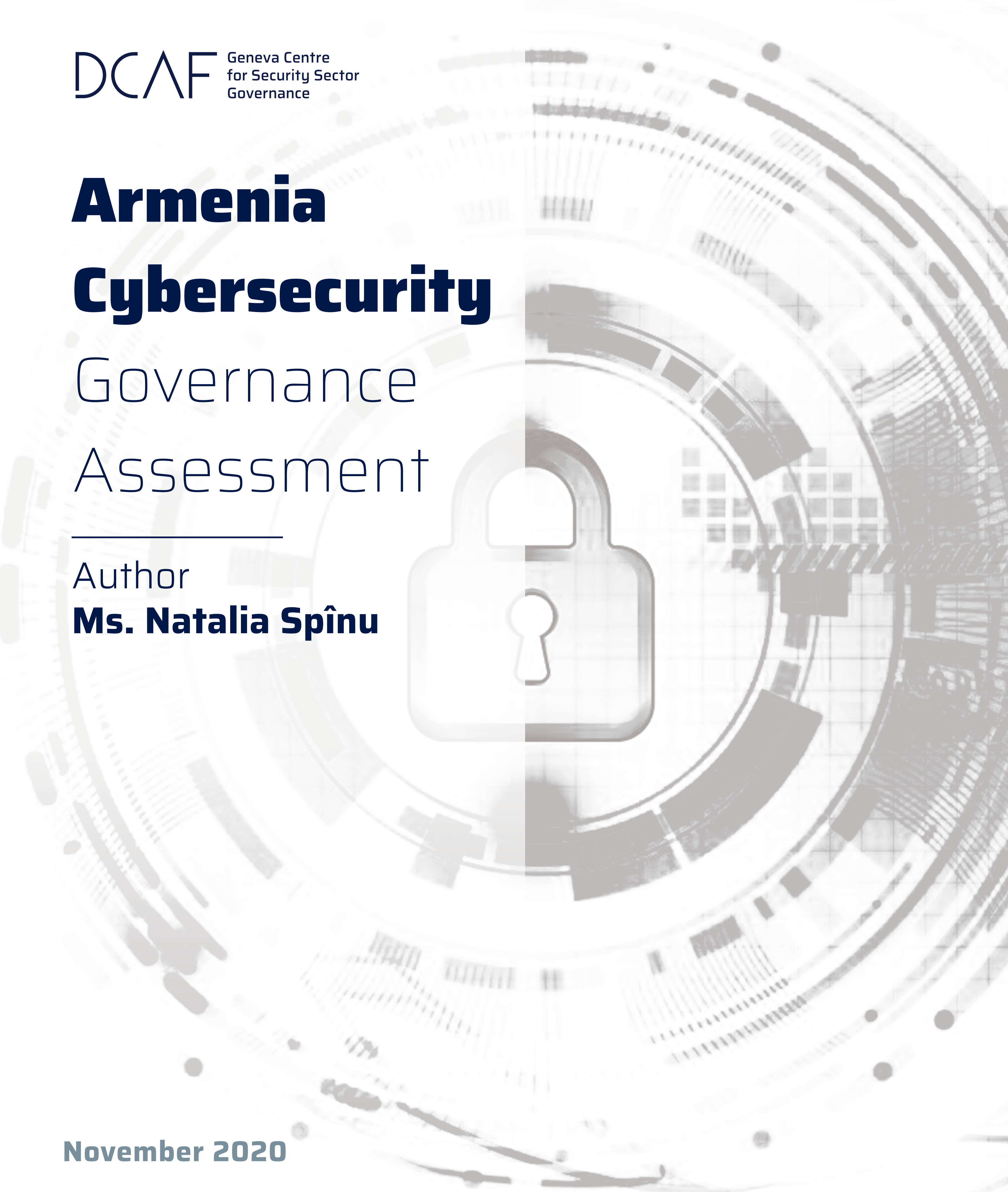
DCAF Geneva Centre
for Security Sector
Governance



Armenia Cybersecurity Governance Assessment

Author
Ms. Natalia Spînu

November 2020

Table of Contents

The Author

Ms. Natalia Spînu is a cybersecurity expert with more than 10 years of work experience in governmental and non-governmental sectors in the Republic of Moldova. She is a member of the Emerging Security Challenges Working Group which operates under the Partnership for Peace (PfP) of Defence Academies and Security Studies Institutes, as well as co-seminar leader of the Program on Cybersecurity Studies from The George C Marshall European Centre for Security Studies, which is tailored for senior officials responsible for developing or influencing cyber legislation, policies, or practices.

At the moment, Ms. Natalia Spînu is the Chief of Governmental CERT in the Republic of Moldova. Under her leadership, CERT-GOV-MD became actively involved in many national cybersecurity development processes, including national cybersecurity program and policy developments, organizing cyber awareness conferences and workshops, building capacity for universities to prepare a qualified workforce for the cybersecurity sector of Moldova, and others. She is responsible for strategic planning and international and intergovernmental cooperation, national cybersecurity policy, international coordination with MFA, and various international projects related to cybersecurity.

As a cybersecurity expert, Ms. Spînu has much experience and is specialized in the following areas: team and project management, ethical hacking, network security, penetration testing and security architectures, cybersecurity program and policy development, audit and implementation of business continuity (ISO-NIST) standards associated with cybersecurity and information security issues, technological risk analysis, etc.

Keywords: cybersecurity, threats, information, Armenia, national strategy, CERT, cybersecurity actors, needs, opportunities.

Summary

This report is a two-factor analysis of cybersecurity, including the legislative framework and key national actors in cybersecurity. The first part of the report presents the main cybersecurity threats in the Republic of Armenia, and the needs arising from national security objectives. The report describes the normative and legislative framework of Armenia, which covers the main aspects of information security ensuring a level of national security of the population, and mentions the main objectives of the national cybersecurity strategy. This report also identifies the issues and challenges in the Armenian cybersecurity strategy, and describes the main actors within the state responsible for the national action plan for cybersecurity. The last part reflects conclusions extracted following the study and elaboration of this report.

Acknowledgements

We would like to express our gratitude to Mr. Grigori SAGHYAN, Manager CERT.AM, Vice President at ISOC Armenia, Associate Professor at the Russian Armenian University, Armenia, who has kindly agreed to discuss a variety of important and specific issues on Armenian cybersecurity. We are deeply thankful for their responsiveness and individual contributions to this report. These insights were useful to draw a parallel between the national situation, the methods applied, and the result obtained. Good practices and examples of different policies addressing national security provided some good insights and perspectives into how to improve the current national cybersecurity strategy of Armenia.

Preface

The power and danger of cyberspace stems from the relationship that information has with the world around it. There are no universally accepted definitions of either cybersecurity or information security. The International Standardization Organization (ISO)[1] defines information security as "the preservation of confidentiality, integrity and availability of information", and defines cybersecurity as "preservation of confidentiality, integrity and availability of information in cyberspace". Meanwhile, the International Telecommunications Union (ITU)[2] does not provide a definition of information security, but rather defines cybersecurity in a lengthy and perhaps all-encompassing way: "The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets".

In recent years, Armenia has seen an unprecedented rise in ICT sector, as more and more people are getting connected to the Internet and the expansion of the 4G network coverage becoming a commonplace phenomenon. Security threats in the modern world often appear in the form of hybrid warfare, including not only military elements, but also the use of economic means, cyber-attacks, fake news, and disinformation. The increasing penetration of information communication technologies (ICTs) into every aspect of society has resulted in both opportunities and challenges.

Concurrently with the development of the ICT sector, the security of the individual, society and the state has become more vulnerable, and therefore needs protection in both the information and cyber domains.

Regarding cybersecurity development, the Global Cybersecurity Index from 2017 shows that Armenia has fulfilled 20% of the cybersecurity criteria. It places Armenia in 110th place in the world in aspects such as ICT development index, networked readiness index, global cybersecurity index, and national cybersecurity strategies. In general, this means that the gap between ICT development and cybersecurity is large.

In recent years, a number of training centres and laboratories have been established, including the Armenian National Engineering Laboratory (ANEL), the Synopsys-Armenia Educational Department, the Armenian Indian Excellence Centre and others. The balanced development of the cybersphere is also in focus as evidenced by the technological centres that have been established in Gyumri and Vanadzor. There has been good progress in the past years in the area of combating cybercrime, where Armenia fulfils 60% of the global index on cybersecurity criteria.

MAIN THREATS AND NEEDS FOR NATIONAL CYBERSECURITY IN ARMENIA

Although Armenia has not published a formal cybersecurity strategy, the National Security Service (NSS)[3] is responsible for cybersecurity policy and the protection of government websites and networks. As mentioned in the strategy, Armenia is an advocate of open, interoperable, reliable, and secure information and cyberspace. Cyberattacks against information resources by foreign states, international terrorist organizations, criminal groups, and individuals threaten Armenia's information security.

The main goal of the policy described by NSS is to balance and protect the interests of the individual, society, and the state. It bases its information and cyberspace policy on the principles of human rights and freedoms, as well as state sovereignty. In the modern world, information wars, including propaganda, manipulations, fake news, and other disinformation tools are becoming more prevalent, and often target democratic values. In this context, Armenia is determined to work to raise public awareness and media literacy to strengthen the capacity of society and the state to counter such information wars.

New and unique challenges have been posed by private entities, including foreign state-funded cyber-attacks which target Armenia's critical information infrastructure and its government structures. In 2013, Kaspersky[4] Lab's Global Research and Analysis Team discovered a large-scale cyber-espionage network which they called "Red October". It was able to infiltrate important state and non-state substructures (including diplomatic, governmental and scientific research organizations in different countries, mainly of Eastern Europe and the former USSR states) and initiate elaborate cyber espionage, even retrieving deleted files in case they were of any interest to the creators of the virus. According to Kaspersky, evidence indicated that the cyber-espionage campaign was active starting from 2007 before being detected in 2013. Armenia made the top ten most infected list with ten cases of infection with the virus.[5]

In 2014 FireEye, an organization that is specialized in information security, exposed the large-scale international activity of a hacker group, with members of the Armenian military among their targets. Fancy Bear hackers had created the fake mail.rnil.am phishing site, imitating the Armenian Ministry of Defence mil.am domain and made it possible to "target members of the Armenian military by hosting a fake login page". It is not clear what damage the hackers had caused in Armenia. In the spring of 2020, European security experts ESET confirmed that numerous websites belonging to the Armenian government have been targeted and compromised by hackers. The compromised websites had been infected with malware and posed a nasty security risk to visitors. It's suspected that the hackers behind this attack were Turla, a Russian hacking group.[6]

In May 2017, the Citizen Lab organization made new discoveries regarding the latest activities of Fancy Bear. This time too, Armenia was on the list of victims. According to the TAINTED LEAKS Disinformation and Phishing With a Russian Nexus[7] report, this time the targets were members of the Armenian government and the military. The report states that Armenia was one of the main targets of the phishing attack, with three percent of the attacks being addressed to the Republic (of Armenia). According to available data, 41 high ranking military officials and diplomats were on the list of Armenian victims. It was also evident that Armenia is a subject of interest in almost all major cyber investigations.

A major challenge in combating threats erupting from cyberspace in Armenia is the imperfection of a comprehensive state policy regulating the information and cybersecurity sector. The absence of proper legislation to ensure the protection of critical information infrastructure, the lack of hardware and human resources dedicated to institutional capacity of computer emergency response teams (CERT), and the absence of a national cybersecurity centre are some of the fundamentals that require attention. In the fields of information, technology, and cybersecurity, Armenia is working to increase the efficiency of institutions and processes, and develop the underlying infrastructure. Armenia plans to develop a legal-normative framework in order to regulate the relationship between the operators of critical information infrastructure, digital service providers, and the state.

Armenia has a variety of e-solutions developed with the support of EU4Armenia: e-Gov Actions (2017-2020) such as e-civil status registry, online business registry, e-penitentiary system, e-apostille, e-draft interactive portal to enable transparent and easy discussion over draft legal acts, and e-request online interactive portal to enable requests, complaints or suggestions to the government, etc. It is vital to continue the developments and adjustments of new e-solutions and technologies to local needs.

To increase resiliency in the cyber space, as mentioned in the National Security Strategy for 2020, Armenia plans to develop national information and cyber capabilities by effectively managing risks, developing qualified professional potential, localizing international standards, and increasing the level of digital literacy.[8] Given the diversity of cyber players, the absence of international borders in the information space, and the involvement of both private and public actors in various capacities, it is crucial to increase the level of cooperation between the public, private, and international sectors in Armenia. Armenia faces a wide range of regional threats - particularly in cyberspace - as a member of both the South Caucasus and the Greater Middle East. Social media have become common vehicles for campaigns to spread false information or fake messages about events, which has been seen in the Karabakh regional context for some time. Armenian digital security expert Artur Papyan, a co-founder of the cyberhub.am civil society media NGO, said that this latest escalation was accompanied by a significant number of cyber-attacks. Coordinated distributed denial-of-service (DDOS) strikes overwhelmed targeted websites with mass bot traffic, while fake accounts bearing Armenian names were created on social media to spread disinformation. Hackers from both Armenia and Azerbaijan defaced each other's websites, displaying nationalistic messages. Mr. Laurence Broers, Caucasus director at peacebuilding NGO Conciliation Resources, said that "The Armenian-Azerbaijani conflict has become highly mediatized, with very substantial social media activity that allows Armenians, Azerbaijanis and others all around the world to participate in localized incidents that become globalized media spectacles with polarizing effects".

In 2016 the Council of Europe's Commission against Racism and Intolerance (ECRI) reiterated its recommendation that the Azerbaijani authorities ensure public officials at all levels to refrain from spreading anti-Armenian statements.[9] ECRI noted that this had been demonstrated in events such as clashes between Armenian and Azerbaijani protestors in the streets of major European cities and even as far afield as Los Angeles.

With regards to protecting critical infrastructure against cyber threats, the Ministry of Transport, Communications and Information Technology elaborated some policies in the reference domain and the implementation of these policies are in-part responsibility of each sector's competent authority such as railway, airway, roadway. The critical infra-

[8] https://mil.am/files/LIBRARY/_pdf_Armenia%202020%20National%20Security%20Strategy.pdf

[9] https://iwpr.net/global-voices/armenia-azerbaijan-clashes-spread-online

structure and any other vital services are subject to the National Security Services protection. They are also in charge of handling and protecting sensitive information.[10]

Globalization as the development cornerstone of a networked society raises the issue of global cyber-security multifold, as vulnerability to global cyber-infrastructure, communication manipulation, under-representation in global cyberspace, crisis of multiculturalism, and international crime and terrorism have multiplied and manifested distinctly in recent years.

In general, it seems that Armenia needs to take a more comprehensive and systematic approach to national cybersecurity development. It would be good to organize a comprehensive cybersecurity management strategy first to define the legal framework, as well as the main stakeholders responsible for the implementation of legislation in the cyber field at the national or at least governmental level. Only after the next steps of paying attention to sectorial capacity development such as private CSIRTs, would SOC teams, departmental CERTs or CSIRTs in the public sector take shape. On both levels, capacity building and expert support in cybersecurity field will be needed.

LAW AND REGULATION IN CYBERSECURITY IN THE REPUBLIC OF ARMENIA

The National Security Council of the Republic of Armenia approved a new National Security Strategy on July 10, 2020.[11] The work on this document has been going on for almost a year. The provisions of the 2020 National Security Strategy clearly set out the fundamental importance of the National Security Strategy (NSS) and the role of the National Security Council apparatus in the policy planning process as well as the rules for reviewing the NSS. The current NSS strategy also focuses on significant issues such as the deteriorating international security environment and hybrid wars which, according to the document, include “not only military elements, but also the use of economic means, cyber-attacks, fake news, and disinformation”.

Meanwhile, in 2020, a draft version of the Cybersecurity Strategy of the Republic of Armenia was developed by the Government of the Republic of Armenia and is still under discussion, the main purpose of which is to define the important elements and key directions of the Cybersecurity Strategy, the necessary measures for sustainable development of the cybersecurity sector and the terms of their implementation, as well as the approaches to the creation of the Cybersecurity Centre.

Regarding international cooperation in cyberspace, Armenia has signed the Budapest Convention on Cybercrime (ETS 185)[12] on 23 November 2001, ratified the document on 12 October 2006, and it entered into force on 1 February 2007. Main threats of cybercrime reported by the counterpart representatives such as the General Department of Fight against Organized Crime of the Police of Armenia, ISOC Armenia, and CERT-AM are hacking, DDOS attacks, malware financial embezzlements, distribution of pornography, and misappropriation of computer data. Identity theft and fake invoice-related frauds are continuously growing (such invoices are being distributed via email to consumers). The Armenian legislation does not include exemptions for the processing of personal data for the prevention, investigation, or prosecution of criminal offenses as included in the Convention 108, article 9 (“the suppression of criminal offences”, and “protecting

[10] https://rm.coe.int/eap-cybercrime-and-cybersecurity-strategies/168093b89c

[11] https://mil.am/files/LIBRARY/_pdf_Armenia%202020%20National%20Security%20Strategy.pdf

[12] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

the data subject or the rights and freedoms of others"), or the EU Directive 95/46 article 13.1. (f) "the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions". Thus, not having an explicit exemption could make the processing of personal data with the purpose to reduce cybercrime more burdensome.

The Armenian procedural legislation contains the notion of "material evidence" which relates to information about the crime, while ISP information that can be collected in the course of an investigation without judicial order is interpreted as "other evidence" or "operational information", and cannot be used as evidence. Evidence cannot be obtained through a voluntary procedure but must be obtained through the legal process for securing evidence.

As an important milestone regarding the countrywide strategic aspect in cyberspace, the National Assembly Standing Committee on Defence in Armenia developed in 2018 a strategic program to fight online gambling. The program also established a strategic program for 2017-2021 for Protecting the Rights of the Child to fight child abuse and child pornography. Currently, the Armenian government is also developing the Digital Armenia 10-year strategy to promote e-government application tools and usage. The fight against cybercrime will notably be a part of this digital strategy. Other aspects include the development of a digital National ID embedded in the SIM card of mobile phones. This Digital National ID could also be used potentially for identification in electronic commerce in addition to identification for government services.

MAIN ACTORS IN CYBERSECURITY IN THE REPUBLIC OF ARMENIA

The main cybersecurity actors in Armenia are the National Security Service, the Ministry of Justice, the Data Protection Authority, the National Communications Regulator, the national CERT - CERT.AM, and ISOC Armenia.

The Ministry of Justice has a main role in developing the legislative framework and the organizational tasks within the government sector regarding codification and legal reforms. The Ministry is also a forum to generate informal cooperation between the public and private sectors. The Prosecutor General's Office has the responsibility to control and to supervise investigative procedures. Cooperation with all national ISPs is considered good, although it was reported that the Office has issues with international providers only. Prosecutors receive technical support from the team of the Investigative Committee, and may involve forensics and other experts. Two prosecutors are specifically dedicated to cybercrime cases.

The High-Tech Crime Department of the National Police is a centralized unit dedicated to handling cybercrimes with a country-wide competency. 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 provides support to local police units. There are different formats in which informal cooperation between police and service providers takes place, such as working group at the National Assembly, non-regular meetings with the providers, Internet Governance Forum-related meetings, etc.

The National Communications Regulator is an independent body, as provided by the Constitution of Armenia. No decision can be approved without the opposition representatives within its board. The entity covers television and radio regulation but has no role on regulating or supervising the Internet. At the same time, a majority of television providers are becoming Internet providers as well (the number of providers is beyond 100), thus legislation is urgently required to follow up this tendency of the market. The Regulator has close contact and cooperation with the police and the Language Inspectorate, but certain government bodies may also have an effect on providers due to industry specific regulations (e.g. advertisements of pharmaceuticals: Ministry of Health). It is the court's competency to decide on breaches committed by providers (fines are imposed generally, but the license may be revoked as ultima ratio).

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 DPA has a staff of 10 persons, including a technical expert for any needed forensics investigations, and the staff is undergoing technical training. Decisions made by the Authority are binding on public and private entities. The Commissioner can receive complaints or open an investigation at its own initiative. The DPA can receive complaints from the public. Complaints have so far not concerned the use of personal data by ISPs or law enforcement authorities, and instead concern the use of personal data for advertising and marketing purposes without the consent of the data subject. The Authority is entitled to impose fines (in the value of 100€ to 1000€) in cases of breaching the relevant regulations.

CERT-AM NREN CSIRT[13] is Armenia's National Research and Education Network (NREN) and Computer Security Incident Response Team. The Acting Head of CERT-AM is Armen Baghdasaryan, and the Deputy Head of Unit is Grigori Saghyan. The team includes five staff members. CERT-AM is sponsored by the Internet Society of Armenia. The establishment of the CERT-AM was mandated via the Internet Society of Armenia decision on 1/09/2007. It collects and analyses 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 evidence about an incident. The preferred method to contact the CERT-AM team for general inquiries is to send an e-mail to the address cert@cert.am which is monitored by a duty officer during hours of operation. It operates 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 maximum commitment to resolve the issues; building on and complementing the existing capabilities in the constituents; fostering a culture of openness within a protected environment by operating on a need to-know basis; and facilitating the exchange of good practices between constituents and peers.[14]

NATIONAL AND INTERNATIONAL COOPERATION ON CYBERSECURITY

Cooperation at the national level between the stakeholders is usually based on personal relationship and trust, documented through bilateral cooperation agreements, in which the official means of communication are negotiated, and the methods used for the exchange of good practices.

At the moment, there are no 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 an informal format, based on personal relations and not within

[13] https://www.cert.am/

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

an 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 an interest to work internationally with the private sector abroad because of the international aspects of cybersecurity. There is also a reported willingness of 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.

Regarding public and private sector cooperation in Armenia, 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. In this framework, parties agreed to communicate in a standardized manner (including cover letters, electronic signatures) and agreed to cooperate in solving issues as soon as possible in case of such procedures. Currently Armenia has no data retention legislation.

Academic institutions play an active role in education on cybercrime; moreover, they also support the work of the police on an occasional basis.[15] 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 being on the topic of cybersecurity and defence. The police support state owned television programs which focus on criminal topics and 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 the police on such topic.

Currently, there is "The Cybersecurity EAST"[16] project, a joint project of the European Union and the Council of Europe. The main objective of EU4Digital initiative is to improve cyber resilience in the six countries of the Eastern Partnership (EaP) region, in line with EU norms and best practices, with a focus on the NIS Directive. The e-Governance Academy (eGA) within the project consults with partner organisations EaP organisations to:

- Strengthen the national cybersecurity governance and legal framework across the EaP countries, in line with the EU NIS Directive;
- Develop frameworks for the protection of operators of essential services and critical information infrastructure in the EaP countries, in line with the EU's relevant policy and legal frameworks;
- Increase the operational capacities for cybersecurity incident management in the EaP countries.

The Armenia-NATO partnership began in 1992, when Armenia joined the North Atlantic Cooperation Council, later renamed the Euro-Atlantic Partnership Council. Armenia is developing policies and capabilities in the area of cybersecurity and is keen to develop cooperation with NATO in this domain. A comparison of the 2009 IPAP and 2014-2016 IPAP demonstrated the positive evolution of cyber cooperation in developing new approach and addressing new elements of cybersecurity. In the framework of the Armenia-NATO Individual Partnership Action Plan for 2017-2019, the 12th "NATO week" events took place in Yerevan in 2019. Public events – conferences, roundtables and panel discussions with active participation of governmental bodies, civil societies, academia,

[15] https://asnet.am/about.php?lang=en

[16] https://eufordigital.eu/discover-eu/eu4digital-improving-cyber-resilience-in-the-eastern-partnership-countries/

NATO international staff and media – took place in the National Assembly of Armenia, in the Ministry of Foreign Affairs and in the Ministry of Defence of Armenia, French and Vanadzor universities.[17]

CONCLUSIONS

All the stakeholders should remember that ICTs are instruments at the service of democratic processes. Information and communication technologies is the rightful combination of online and offline tools contributing to a successful cybersecurity approach by raising cybersecurity awareness, promoting cyber hygiene among citizens, as well as setting a legislative framework in the field that will ensure the needs of society. This starts with the establishment of a National Cyber Strategy for the coming years and investing resources in hardware and software for cyber exercise centres dedicated to incident response practice for the public sector. Demonstration of the cybersecurity utilities should be created by providing evidence to the population.

Today, the world faces a dramatic increase in violence in all spheres of life, and particularly in cyberspace. The South Caucasus is one of the most militarized regions in the world, where the lack of a culture of peace makes the region a potential powder keg. That's why it is essential to establish a human-centric cybersecurity architecture and sustainable development focused on cooperation instead of confrontation. Stakeholders from the public and private sectors have a more or less uniform opinion with regards to the best strategy that Armenia should pursue for a better cybersecurity infrastructure in the country, with the following set of focus areas:

- Clear legislation setting out the procedures and rules for access to data held by Internet service providers, based on the standards of the Council of Europe/Budapest Convention;
- Identification and engagement of all possible parties – governmental, non-governmental and business into the multi-stakeholder process of cooperation;
- Building an understanding of common interest and values for the security of Armenian citizens in cyberspace and facilitating voluntary compliance to best practices (e.g. reporting, awareness, prevention);
- Ensuring that cooperation with foreign/multinational ISPs 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 private cybersecurity structures to be set up (private CERTs, CSIRT) which could be useful filling gaps in expertise of public institutions caused by the difficulty of maintaining good experts, as the offer on the private market is substantially superior.

[17] https://www.mfa.am/en/international-organisations/3

DCAF Geneva Centre for Security Sector Governance

DCAF Geneva Headquarters

P.O.Box 1360
CH-1211 Geneva 1
Switzerland

✉ info@dcaf.ch
☎ +41 (0) 22 730 9400

www.dcaf.ch

@DCAF_Geneva