DCAF Geneva Centre for Security Sector Governance

Azerbaijan 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 Cyber Security Studies from The George C Marshall European Centre for Security Studies, a program which is tailored for senior officials responsible for developing or influencing cyber legislation, policies, or practices.

At the moment, Ms. Natalia Spînu is 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 cybersecurity sector of Moldova, and others. She is responsible for strategic planning and international and intergovernmental cooperation, national cybersecurity policy, and international coordination with MFA and International Projects on various tasks related to cybersecurity.

As a cybersecurity expert, Ms. Spînu has 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, Azerbaijan, 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 Azerbaijan and the needs arising from national security objectives. The report describes the normative and legislative framework of Azerbaijan which covers the main aspects of information security in cybersecurity and ensures a level of national security of the population, while mentioning the main objectives of the national cybersecurity strategy. The last part reflects the conclusions that we have extracted following the study and elaboration of this report.

Acknowledgements

We would like to express our gratitude to Mr. Tural Mammadov, OIC-CERT Board Member, CISO at SASCIS (SSPS), and Adviser to Cybero Ltd., Azerbaijan, who accepted to discuss a variety of important and specific issues, for their responsiveness and individual contributions to this report. I very much appreciate the valuable contribution received. His answers were useful in order to draw a parallel between Azerbaijan's national situation, and to contrast the methods applied versus the result obtained.

Preface

Azerbaijan, a state which is located at the crossroads of Europe and Asia, is surrounded by the Caspian Sea and Caucasus mountain range. The disputed region of Nagorno-Karabakh, its recent escalation and the international armed conflict it brought, the energy security of the Caspian Sea, the antagonistic neighbouring states of clerical Iran and nuclear Russia, and traditional security, have always been key influencers of Azerbaijan's foreign and domestic policies. Stuxnet, a computer worm attack[1], dragged the attention of the country toward cybersecurity awareness, as it did in many other affected states in the world. Though Stuxnet has mainly targeted Iranian computers, it has been spotted in some other states including Azerbaijan. No doubt the prompt reaction of effective antidotes overcame the limited damage of this "cyber-missile", but the Stuxnet incident alarmed the existing safeguards of cyberspace in Azerbaijan. Moreover, authorities of the country faced the investigation of the origins of 25 cyber-attacks in 2012: 24 originating from Iran and one from Netherlands. Therefore, cybersecurity has become one of the more serious concerns and challenges to the national security of Azerbaijan.[2]

CYBERSECURITY IN AZERBAIJAN

Azerbaijan has been exposed to the relentless growth of cybercrime and information security-related threats and offences in last three years. For example, in the period from January through September 2019, 42% of PC users in Azerbaijan faced cyber threats, with many users exposed to threats of the spread of malware (software) to data storage devices like memory cards and hard drives. The encryption and threat programs have also intensified over the past period. Kaspersky (Internet security software) detected about 7,500 of malicious programs in the middle of 2019 (in the second quarter) and prevented 388,000 attempts to direct Internet users of the Azerbaijani segment to phishing websites.[3]

The most representative cause, which is found in many other developing countries, is that Azerbaijan is becoming increasingly dependent on the use of services and applications provided by information and communication technologies (ICT) and has not been adequately equipped to safeguard its interests that are by-products of intensive use of ICT. Secondly, the ongoing Nagorno-Karabakh conflict, which became a serious geo-political conflict in the second half of 2020, has made cybersecurity in Azerbaijan more vulnerable.

In the first quarter of 2020, Azerbaijan entered the top-10 list of the countries exposed to the attack of the Ciphering-Trojan password-stealing malware. From January to March, miner attacks in Azerbaijan accounted for 1.21%, attacks of web-malicious software for 6.49%, and local infection attempts for 33.88%. In the reporting period, countrywide attempts of infection with mobile malicious software accounted for 2.68%, mobile bank threats accounted for 0.06%, and mobile invader Trojan threats accounted for 0.01%. Furthermore, 1.4% of user devices were exposed to attacks of malicious bank software during this period.

In the spring of 2020, a threat actor targeting Azerbaijan showed an interest in the energy sector; specifically SCADA systems related to wind turbines. The attacks were aimed at both government organizations and private sector companies, and most of these attacks involved a remote access Trojan (RAT) that has not been seen before. According to Talos[4], the hackers appeared to be interested in the energy sector and industrial control systems (ICS).[5] Lately, in autumn of 2020, unidentified spies have been quietly breaching Azerbaijani government IT networks and accessing the diplomatic passports of certain officials, according to new research from Talos, Cisco's threat intelligence unit.[6]

These statistics are proof that Azerbaijan is targeted for cyber-attacks and demonstrate that there is a lack of cybersecurity responsibility for digital web providers, as government doesn't have a competent authority in the field of cyber/information security that has the power to supervise public and private digital service providers regarding the implementation of cyber/information security requirements.

The government of Azerbaijan is rapidly developing its e-infrastructure with the help of ANAS (Azerbaijan National Academy of Science)[7] and improving the digital infrastructure of the state. Such an emerging digital environment needs a fool-proof communications network system. Cybersecurity is critical in many fields such as administrative, technical, sociological, historical, legal, political, military and academic. Handling cybersecurity issues in a comprehensive manner with a wholistic approach is possible only by determining the principles and strategies that are targeted at addressing each domain and thematic of cybersecurity, as well as cybersecurity as a single structural entity.

MAIN LEGAL AND POLICY DOCUMENTS GOVERNING CYBERSECURITY

The legal basis of cybersecurity needs to be strengthened in Azerbaijan, because cyber weapons in different forms (such as the Stuxnet virus) have already attempted to destroy the government cyber infrastructure. There is an urgent need for a strong and well-secured cyber network to prevent the risks of cyber-attacks in the digital infrastructure of the country. Furthermore, the promotion and advancement of cyber laws with the establishment of a cyber army has become a vital demand for Azerbaijan in order to strengthen the national cybersecurity of the state. In this way, the safety and security of cyberspace is a question of immense importance for Azerbaijan, because the growing dependence of industry, government and financial institutions on cyber networks needs a completely secured and reliable information system, which could maintain cyber deterrence in the global cyberspace. At the moment, there are some national laws related to cybersecurity as well as some international directives in effect:

- Law of the Republic of Azerbaijan on Legal Protection of Databases (2004/09/14)[8]: the present Law regulates legal relations arising from the creation and use of compilations of data irrespective of their forms.
- Law of the Republic of Azerbaijan on approval of Convention of Budapest "On Cybercrime"[9]
- Law of the Republic of Azerbaijan on Information, Informatization and Protection of Information (1998/04/03)[10]: it regulates relations arising from formation of information resources based on the creation, collection, processing, accumulation, storage, search, dissemination of information, establishment and use of information systems, technology, and means for their insurance and at protection of information. The Law shall establish the rights of subjects involved in information processes.
- Law of the Republic of Azerbaijan on the Right to Obtain Information (2005)[11]. The purpose of the present Law is to establish the legal framework for ensuring free, unrestricted and equal information access as prescribed by Article 50 of the Constitution of the Azerbaijan Republic, based on open society and democratic law-governed state principles, as well as to create conditions for control by citizens on the exercising of public duties.
- Criminal Code of the Republic of Azerbaijan (excerpts)[12].
- National Security Concept of the Republic of Azerbaijan adopted by the Decree 2198 of the President on May 23, 2007, and the Decree of the President of the Republic of Azerbaijan 'On measures for ensuring information security in the state bodies of the Republic of Azerbaijan'[13].

8 https://www.legislationline.org/download/id/4292/file/Azerbaijan_law_legal_protection_of_compilations_of_data_2004_en.pdf
9 https://mincom.gov.az/upload/files/9dd20fa1b4035d04117ea2e286a26bfc.pdf
10 http://www.legislationline.org/documents/action/popup/id/6959
11 https://www.legislationline.org/download/id/3844/file/Azerbaijan_Law_on_right_to_obtain_information_2005_en.pdf
12 http://www.legislationline.org/documents/action/popup/id/17617
13 https://www.files.ethz.ch/isn/154917/Azerbaijan2007.pdf

- National strategy for the development of the information society in the Republic of Azerbaijan for 2014-2020 approved by the Order of the President of the Republic of Azerbaijan (2014/04/02)[14].
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)[15].
- Decision of the Cabinet of Ministers of the Republic of Azerbaijan on approval of the "List of information systems and resources to be connected to E-government portal" and "Technical Requirements for connection of information systems and resources, e-services to E-government portal"[16].

Azerbaijan is taking several initiatives and constructive steps for the protection of its digital infrastructure. The minister of Communication and Information Technology has repeatedly highlighted the vision of the government in a statement to strengthen Azerbaijan's information security. Moreover, he has also highlighted and mentioned the ambition of his country for the development of an international collaboration against the prevailing threats of organized cyber-attacks.

No doubt, a multilateral cooperative approach could augment the existing laws of cybersecurity, but the active individual efforts of states could play a more effective role as well. Therefore, the combination of unilateral and multilateral approaches is being sought to counter the overwhelming non-military and transnational threats of cyber-attacks.

Controlling crime in Azerbaijan has been widely seen as the sole responsibility of public law enforcement agencies, meaning that the state is accorded wide powers to enforce its positive obligation to protect individuals and their rights against crimes and bring offenders to justice. An essential role is still expected to be performed by public law enforcement agencies in ensuring cybersecurity, but the limitations of the configuration of ICT mean that apprehending and prosecuting offenders is not enough, and attention has to be paid to a full array of strategies – the 'Four Ps' approach (Prepare, Prevent, Protect and Pursue).

National cybersecurity strategy

Azerbaijan currently has a strategy on cybersecurity for 2014-2020, which was approved by the Order of the President of the Republic of Azerbaijan (2014/04/02) and is based on the "National Strategy for Information and Communication Technologies for the Development of the Republic of Azerbaijan (2003-2012)" approved by the Decree of the President of the Republic of Azerbaijan No. 1146 dated February 17, 2003. The state also adopted a cybersecurity strategy in connection with the implementation of this National Strategy for ICT. The National Strategy for ICT created the foundations of information society in Azerbaijan, addressing the widespread use of ICT by its citizens, society, and the private sector; and government agencies created favourable conditions for planning activities in the next stage. Azerbaijan society's need for modern communication and new information technologies in order to gain global experience, interaction and cooperation with international organizations has been met.

14 https://president.az/articles/11312
15 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148&qid=1609855280441
16 https://mincom.gov.az/upload/files/61904ecacaa5ed89ae7e53857166644a.pdf

During these years, an appropriate legal framework has been created to ensure development in the field, and many important laws and other normative legal acts have been adopted.

State programs for the development of communication and information technologies in the Republic of Azerbaijan were approved by the relevant decrees of the President of the Republic of Azerbaijan in 2005 and 2010, as well as the Cabinet of Ministers of the Republic of Azerbaijan dated May 14, 2010 No. 136s. In 2011, the "Action Program for the Formation of e-Government" provided for the implementation of practical measures related to the development of ICT.

These legal acts, along with the opening-up of new opportunities for the development of ICT in Azerbaijan, have created conditions for the observance of the principles of free market and healthy competition in the IT field and the widespread use of ICT by citizens and government agencies.

In recent years, the ICT sector has become a leading and dynamically developing sector of the economy. The IT sector's volume has doubled every three years, with an average annual growth rate of about 20-25%, exceeding $ 1.9 billion, with a share of 1.7% in GDP and a share of non-oil GDP of 3%. Investment in the IT sector amounted to about $ 2.5 billion, of which 28% was invested by the state and 72% by local businesses and foreign investors. The share of the private sector increased from 67.3% to 80% compared to 2003. According to the results of 2013, 70% of the population of Azerbaijan are Internet users, including 50% of them which are broadband Internet users. Over the past five years (2014 to 2019), the capacity of the international Internet channel has increased 12.9 times to 200 Gbit/s, and the volume of the Internet services market has increased almost four times.

One of the aims and main tasks of the National Strategy is ensuring the security of the country's information space, increasing confidence in the use of ICT, developing the regulatory framework governing this area, and the implementation of information and awareness are the main objectives of this strategy. In order to achieve the goals of this strategy, the following policy guidelines are envisaged:

- improvement of a unified state policy and legal framework in the field of information security;
- development of the national information space and critical infrastructure of the country, as well as the system ensuring information security of the information infrastructure;
- implementation of measures to reduce technical and technological dependence on foreign relations in the country's information relations;
- ensuring information security of "e-government" infrastructure;
- implementation of information on electronic threats at the national level;
- creation of appropriate technical and methodological tools, development of recommendations and provision of methodological support in the field of strengthening cybersecurity;
- development and application of "safe Internet" mechanism to protect children from illegal and dangerous content;
- coordination of activities of state and non-state information infrastructure entities on cybersecurity;

- education of the population, private and other institutions in the field of cybersecurity and formation of information security culture, training of qualified personnel in this field;
- ensuring international cooperation in the field of information security of the country.

In the process of implementing the National Strategy, close cooperation and coordinated activities between government agencies, the private sector and civil society institutions are ensured, and active propaganda is carried out for the wide dissemination of information society ideas. A new strategy for the future years is being developed under the supervision of the Head of the Department of Innovative Development of Information Society and Electronic Governance.

MAIN ACTORS IN CYBERSECURITY IN AZERBAIJAN

According to the Computer Incident Response Team (CERT) at Azerbaijan's Special Communication and Information Security State Agency, the number of computer security requests from the country's government agencies exceeded 1,200 in January-April 2019, a 34.1% increase on the same period last year[17]. Three major institutions of government are involved in the defences of Azerbaijan's cyber borders: the Ministry of Communication and Informational Technology (MCIT), the Ministry of National Security (MNS), and the Azerbaijan National Academy of Sciences (ANAS) through its Information Technologies Institute (ITI). To safeguard computer networks across the Government departments of Azerbaijan, a computer emergency response team CERT-GOV-AZ[18] has been created under the Special State Protection Service to respond to information security incidents. There is also an Electronic Security Service under MTCHT which acts as a certification body. A cybersecurity strategy is also under preparation, and the MTCHT intends to implement a cyber operation centre for real-time monitoring of cyber threats.

The Ministry of Communication and Information Technologies of Azerbaijan is a central executive body implementing state policy and regulation in the areas of transport including maritime transport and civil aviation; communications (telecommunication, postal services); and high technologies (information technologies, microelectronics, nano, bio and other innovative science-intensive technologies). In its activity, the Ministry is guided by the Constitution of the Republic of Azerbaijan, international treaties to which Azerbaijan is a signatory, laws of the Republic of Azerbaijan, decrees and orders of the President of the Republic of Azerbaijan, decisions and resolutions of the Cabinet of Ministers of the Republic of Azerbaijan, and these Regulations.

The Ministry progressed in facilitating public access to government services through the ASAN[19], a state agency for public services to citizens of Azerbaijan. "ASAN service" centre under the State Agency for Public Service and Social Innovations under the President of the Republic of Azerbaijan was established by the Decree of the President of the Republic of Azerbaijan No.685 dated 13 July 2012.

Currently 450 e-services are being provided through this e-government portal. To continue this mission of e-governance, the government, intends to intensify work related to:

(1) establishing an e-Government Academy;

17 https://eufordigital.eu/azerbaijan-develops-strategy-for-cybersecurity/
18 https://cert.gov.az/en/pages/3
19 https://www.asan.gov.az/en

(2) establishing an e-Government Research Centre;

(3) capacity building and knowledge-sharing on e-Government; and

(4) development of e-Government infrastructure (implementation of a government cloud called G-Cloud).

The Ministry of Transport, Communications & High Technology is appointed as the operator of G-Cloud and is tasked with organizing the storage in the data centre, the state information systems and reserves of governmental bodies, legal entities in state ownership, as well as legal entities with a controlling stake run by the government, budget organizations, public legal entities, and ensure the use of G-Cloud by them. The Special Service of State Protection is commissioned to provide governmental bodies with the necessary telecommunication channels for their connection to G-Cloud.

The Cyber Security Centre (CERT.GOV.AZ) is established under the Ministry of Communication and Information Technologies of the Republic of Azerbaijan in accordance with part 5 of decree 708 of the President of the Republic of Azerbaijan, dated 26 September 2012. It operates with the authority delegated by the Special Communication and Information Security State Service of the Azerbaijan Republic. The Centre has no powers to stop criminal activity, but reserves the right to transfer consideration to corresponding law enforcement bodies. The Centre is a state coordinating body which engages in coordinating the action of information infrastructure subjects, reporting about existing and potential risks at country level, educating the public, private and other institutions in the field of cybersecurity, and providing methodological assistance to them. CERT.GOV.AZ operates to support the following computer incidents. Support level depends on incident and its type and is determined by members of group:

- Violation of working potential of basic nodes of a network and resources of large servers, and attacks which can cause crash of the system information;
- Network attacks directed on obtaining (increase) of privileges;
- Attacks such as DoS (Denial of Service) and DDoS, directed on information resources of state structures and separately taken hosts;
- Purposeful sending of viruses; destruction of systems of protection of information networks, including application of harmful programs (sniffer, rootkit, key logger etc.);
- Scanning of national information networks and hosts;
- Search or interception of passwords and other authentication information;
- Unapproved usage of information resources.

The Electronic Security Service (ESS) under the Ministry of Communications and High Technologies (MCHT) was established pursuant to the 5th part of the Decree of the President of the Republic of Azerbaijan № 708, dated September 26, 2012. By Decree of the President of the Republic of Azerbaijan on additional measures to improve management in transport, communications and high technologies field, dated January 12, 2018, the Centre was included in the structure of the Ministry of Transport, Communications and High Technologies as the ESS. The ESS is a coordinating state authority, which provides information on infrastructure, awareness about existing and potential e-dangers at the country level, education of the population, private entities and other organizations in

the field of cybersecurity, and also provides methodical assistance[20]. The ESS carries out the following activities:

- to coordinate the activity of entities of information infrastructure in the area of cybersecurity;
- to collect and analyse information from users, manufacturers of software, hardware and technical equipment, analogical structures in foreign countries and other sources about cyber-attacks, trespassing, malicious computer programs (hereafter referred as electronic threats of danger) directed against the security of information systems and networks, computer equipment and their software, and local and corporative information systems and resources;
- to carry out notification of existing and potential cyber threats in order to raise awareness of users on issues of cybersecurity;
- to prepare instructions and recommendations about the programs and technical facilities threatening users, and provide methodological support to counter cyber threats;
- to implement preventive measures in collaboration with the national Internet operator and MTCHT to repel cyber-attacks in the global Internet traffic;
- to cooperate with other relevant bodies operating in the country to provide preparedness for the cybersecurity.

Azerbaijan National Academy of Sciences (ANAS) and its Information Technologies Institute (ITI):

in 2002, the Institute of Information Technology was founded within the Information and Telecommunication Scientific Centre (ITRC). In a short period of time, the institute transformed itself into an organization conducting innovative scientific research on the contemporary problems of ICT. Thus, the studies on actual scientific and theoretical problems of information technology and information society were founded, and new research departments and centres opened. The institute is a scientific body, where important projects are implemented, and all the facilities meeting international standards are provided to achieve efficient research results and to organize higher innovation activity for the organization. The institute implements successful work towards the implementation of scientific, technical and innovation policy. The main objectives of the institute include the organization and development of scientific activities in accordance with modern requirements with the use of a wide range of ICT opportunities, improving scientific governance, forming national scientific information space, integrating into the international scientific environment, and high-level personnel training[21]. Significant scientific achievements of the institute are:

- An optimal authentication system distributed by value and time indicators were developed for adaptive networks; and a theoretical game model was proposed for decision-making in the fight against the various threats in corporate networks. The models were proposed for the detection of information security threats in computer networks, and for information security risk assessment and control.
- Methods and algorithms were developed for the detection of information warfare manifestation in the virtual environment. The models and methods were proposed

[20] https://mincom.gov.az/en/view/organization/17/
[21] https://ict.az/en/content/250

for e-science formation, management and assessment in the republic, and for information security support; numerous conceptual approaches were proposed for the establishment and improvement of AzScienceNet and for adapting its characteristics and quality indicators to European standards; several approaches and methods were developed for the detection and analysis of social networks in e-government, secret protection, process monitoring and assessment, security provisioning, and intelligent analysis of personal data.

- Methods and algorithms were developed for the intelligent analysis of Big Data (Data Mining). Multiple methods and algorithms were proposed for grouping the sets of text documents by their content, for their automated summarization, and for assessment of summaries (Text Mining).
- Cryptographic methods and algorithms based on the elliptic curves over finite fields were developed for the creation of e-signature infrastructure. Numerous methods and algorithms were developed for the establishment of biometric identification systems and their security assessment, as well as for biometric template protection and the interoperability of biometric sensors. A method of biometric cryptosystem synthesis was proposed by the unification of the advantages of biometric technologies and asymmetric cryptographic systems; methods and algorithms were developed for the human face recognition according to photo portraits.

The National Bank of the Republic of Azerbaijan (CBA) provides: goals, functions and authorities, as well as management and organizational structure of the bank and its relations with public authorities and other persons. The banking sector necessitates maintaining information security, protection of information resources in use from possible threats, boosting overall cybersecurity readiness and regular awareness efforts during data sharing. The CBA is developing new standards for information technology and IT security.[22]

Although some organizations created security operations centres, Azerbaijan is still in need of a national security operations centre to monitor and secure general Internet traffic in Azerbaijan, monitor real-time attacks, and provide an overall cybersecurity architecture in Azerbaijan. The National Cybersecurity Service of Azerbaijan includes penetration testing, malware analysis, incident response, attack examinations and other services for private companies, banks, financial organizations, and public agencies under the Ministry of Transport, Communications and High Technologies. It is continuously investing in additional trained resources and specialists in cybersecurity.

NATIONAL, REGIONAL AND INTERNATIONAL COOPERATION AMONG CYBERSECURITY STAKEHOLDERS

Cybersecurity organizations and Internet service providers constructed their security infrastructure over the last five years.

Partnership of Azerbaijan, Georgia, Moldova and Ukraine within the organization "For democracy and economic development – GUAM"[23] is an example of regional coopera-

22 https://en.azvision.az/news/129663/central-bank-of-azerbaijan-developing-new-standards-for-it-security%C2%A0.html

23 https://guam-organization.org/en/about-the-organization-for-democracy-and-economic-development-guam/

tion. Partnership with Ukraine and Moldova is not confined only to the GUAM framework, but at the same time is framed on developing on a bilateral basis a secure cybersecurity net in political, economic, humanitarian and other spheres. GUAM main goals are strengthening democratic values, ensuring the supremacy of law and respect for human rights, ensuring sustainable development, strengthening international and regional security and stability, deepening European integration for the creation of a common security space and the enlargement of economic and humanitarian cooperation, developing socio-economic transport, energy, scientific, technical and humanitarian potential, and stimulating political interaction and practical cooperation in fields of mutual interest.

Currently, Cybersecurity EAST[24] (EU4Digital) is a joint project of the European Union and the Council of Europe. The main objective of the EU4Digital initiative is to improve cyber resilience in the six countries of the Eastern Partnership (EaP) region, and functions in line with EU norms and best practices with a focus on the NIS Directive. e-Governance Academy (eGA) within the project consults with EaP partner organizations 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 EaP countries.

In addition, Azerbaijan has been actively engaged within the framework of the NATO[25] Science for Peace and Security (SPS) Programme since 1995. The NATO SPS Programme enables close collaboration on issues of common interest to enhance the security of NATO and partner nations by facilitating international efforts to meet emerging security challenges, support NATO-led operations and missions, and advance early warning and forecasting for the prevention of disasters and crises. The Programme also helps to prepare interested eligible nations for NATO membership. Recent leading areas of cooperation included Cyber Defence, Counterterrorism, and Disaster Forecasting and Prevention. The SPS programme organized two Advanced Training Courses (ATCs)[26] on cyber defence for Azerbaijani civil servants holding key roles in cybersecurity in September 2018 and December 2019 in Baku. The ATCs provided advanced training on operational cybersecurity and cybersecurity technology content to ensure cyber resilience in Azerbaijan. These tailor-made courses imparted information on advanced cybersecurity concepts, best practices and experiences at the international level. All lectures focused on Azerbaijan's cybersecurity and its defence needs, and were complemented by laboratory sessions. These activities were led by experts from Azerbaijan and Turkey.

CONCLUSIONS

At the moment, Azerbaijan has a gap between ICT development and cybersecurity development; the state needs to pay attention to minimize it. Good progress has been made in the cyber threat analysis area, as well as in the electronic identification and electronic signature domain. There is now an important requirement to put emphasis on more homogenous development of e-services. Currently the accessibility and quali-

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

[25] https://www.nato.int/cps/en/natohq/topics_49111.htm

[26] https://www.nato.int/cps/en/natohq/news_166934.htm?selectedLocale=en

ty of e-services is uneven. For a better transition from offline to online service delivery to happen, it is necessary to ensure the support from legal and institutional entities as well as redesigning processes. A suggestion for the e-governance transition process is to develop services and solutions that ensure Security by Design to minimize the risks of security breaches and vulnerabilities. It is cheaper and easier to design systems from the start that take into account the present legal framework in ICT and cybersecurity.

When analysing the threat background, the cybersecurity strategies of the past decade and the actual legal framework in the country, it is crucial to take some serious steps to ensure the continuity of e-transformation and e-governance in Azerbaijan that will fulfil the requirements and needs of current day cyber-landscape.

Malware operators have been observed evolving their tactics to hack into sensitive targets. Previous campaigns have been focused on the energy sector, especially wind turbines. The September and October campaigns in 2020 were focused on the public sector and VIPs. Moreover, the campaigns launched are increasingly efficient and have become difficult to detect due to obfuscation techniques. That's why securing SCADA systems and other types of industrial control systems (ICS) should be made a priority of the cybersecurity governance in Azerbaijan. In addition, it is necessary to better establish public-private cooperation and to designate authorities to monitor cybersecurity matters on telecommunication and the Internet, as many attackers exploit the vulnerabilities and lack of preparedness of citizens and disable as many resources as possible.

The Azerbaijan public sector and other important organizations are still targeted by new versions of PoetRAT[27]. That's why it is important to raise awareness about ways to prevent cyber espionage, spear-phishing attacks, and to focus on easy and accessible ways of combating these attacks of criminal design. National-level workshops and practical exercises will also be effective at presenting the countermeasures, especially for law enforcement departments and incident response teams. Techniques and tools to promote essential cybersecurity skill sets and knowledge among citizens should be promoted, as should mass media campaigns on identification and reporting of cyber incidents. Azerbaijan should measure its cyber threats through the financial lens of impact and invest in those cyber countermeasures that are the most critical, such as: cybersecurity of ICS systems, network security, and enhancement of public employees cybersecurity skill sets.

Strong cybersecurity is linked to technology, but also greatly depends on the political or cultural will in every country, and hinges on the level of societal involvement and its openness. There are many ways in which a country can improve its cybersecurity resilience, which is why it depends on national strategies and the willingness of the governance to develop the correct cybersecurity landscape. All available measures require resources such as hardware and software, cybersecurity experts and time.

[27] https://blog.talosintelligence.com/2020/10/poetrat-update.html

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