DCAF Geneva Centre for Security Sector Governance

Ukraine Cybersecurity Governance Assessment

Author
Ms. Natalia Spînu

November 2020

Table of Contents

About DCAF

The Geneva Centre for Security Sector Governance (DCAF) initiated by Switzerland, is an international foundation established under Swiss law, making states and people safer within a framework of democratic governance, the rule of law and respect for human rights. DCAF has been implementing successful cybersecurity research and capacity-building projects in Southeast Europe for the past six years.

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, international coordination with MFA, and various international projects 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: cyber security, threats, information, Ukraine, national strategy, CERT, cybersecurity actors, needs, opportunities.

Summary

This report is a two-factor analysis of cybersecurity: the legislative framework, and key national actors in cybersecurity. The report describes the main cybersecurity threats in Ukraine and the needs arising from its national security objectives. The present assessment paper describes the normative and legislative framework of the Ukraine, which covers the main aspects of information security and ensures a level of national security of the population, while mentioning the main objectives of the national cybersecurity strategy as well as the main actors and stakeholders in the national cybersecurity.

Acknowledgements

We would like to express our gratitude to Ms. **Yevheniia IVAKHNENKO**, state expert, Department of information security and cybersecurity at the National Cybersecurity Coordination Centre at NSDC of Ukraine (The National Coordination Centre for Cybersecurity under the National Security and Defence Council of Ukraine), who accepted to discuss a variety of important and specific issues, for their responsiveness and individual contributions to this report. We very much appreciate the valuable contribution received. Her answers were useful for us to draw a parallel between the national situation and the methods applied versus the result obtained. Good practices and examples of different policies to address national security gave us good practices and perspectives to improve our current national strategy and tools of work.

MAIN CYBERSECURITY THREATS AND NEEDS IN UKRAINE

In response to large-scale attacks to its critical infrastructure, Ukraine adopted in 2016 a National Cybersecurity Strategy and is making strides in its implementation. The set-up of the National Cybersecurity Coordination Centre in 2016 and the proposed update of the cybercrime legislation to meet the Budapest Convention requirements and best practices, particularly on Internet Service Providers, are some main steps in enhancing the country's cyber resilience. These activities are complimented by strong cooperation with international partners across the cyber sphere, including on cybercrime and cyber defence. Threats to cybersecurity according to the National Cybersecurity Strategy[1] are actualized through the following factors, in particular:

- Dissimilarity of national electronic communications infrastructure, its development and protection level to modern requirements;
- Insufficient level of protection of critical infrastructure, public electronic information resources and information, since the requirement of information protection was imposed by law, from cyber threats;
- Unsystematic cyber protection measures of critical infrastructure;
- Ineffective activities of the security and defence sector of Ukraine in combating cyber-threats of military, criminal, terrorist and other natures;
- Inadequate level of coordination, cooperation and information exchange among the cybersecurity entities.

It is possible to utilize the Strategy's approaches to attempt to classify threats to the cybersecurity of Ukraine. The threats may be divided into three broad categories:

1. Threats aimed at cyber defence - actions directed at key infrastructure or informational resources (regardless of the actor, be it a hostile state, a "hacktivist" organization, a terrorist group, etc.);
2. "Generic" cybercrimes (aimed mainly at interests of private entities and not the society in general);
3. Threats to cyber resilience (non-intentional cyber incidents).

Ukraine is also in need of proper regulatory governance of the public-private partnership mechanisms for Critical Infrastructure Protection (CIP). It requires development of a legal framework for mutual obligations of the state and non-government subjects in respect of CIP[2], for the implementation of risk analysis and contingency planning practices, as well as mechanisms and tools for coordination between government and non-government subjects and the public, and the responsibility sharing mechanisms (including in respect of financial responsibilities) in the activity of business entities.

There are several areas in cybersecurity that need more resources and immediate involvement in Ukraine, such as the lack of cyber crisis management exercise with cyber components, as well as a cyber-crisis management plan. The Ukraine government must establish a comprehensive crisis plan for large-scale cyber incidents. Different components of a crisis plan must be established by legislation. Ukraine also needs the capacity

[1] https://thegfce.org/cybersecurity-in-ukraine-national-strategy-and-international-cooperation/
[2] http://old2.niss.gov.ua/content/articles/files/niss_Engl_findruk-0e9af.pdf

to conduct military cyber defence operation starting with operation planning units, operational exercises and participation in international cyber operation exercises in order to develop skills and good practices in the service of national strategy threats and needs.

With regard to research and scientific aspects, Ukraine is severely lacking efficient specialized research institutions in the cybersecurity area. At the same time, it is worth noting that these problems are not intrinsic only to Ukraine: questions of the functioning of public-private partnerships are debated even in states with the most developed legal systems.

MAIN LEGAL AND POLICY DOCUMENTS GOVERNING CYBERSECURITY

- Law of Ukraine "On Basic Principles of Cyber Security of Ukraine", which defines the legal and organizational basis for protecting the vital interests of man and citizen, society and state, the national interests of Ukraine in cyberspace, the main goals, directions and principles of state policy in cybersecurity, state powers bodies, enterprises, institutions, organizations, individuals and citizens in this area, the basic principles of coordination of their activities to ensure cybersecurity;[3]
- Order of the State Special Communications Administration dated 10.06.2008 № 94, which approved the "Procedure for coordinating the activities of public authorities, local governments, military formations, enterprises, institutions and organizations, regardless of ownership, to prevent, detect and eliminate the consequences of unauthorized actions against state information resources in information, telecommunication and information-telecommunication systems";[4]
- Resolution of the Cabinet of Ministers of Ukraine of 16.11.2002 № 1772, which approved the "Procedure for cooperation of executive authorities on the protection of state information resources in information and telecommunications systems";[5]
- Resolution of the Cabinet of Ministers of Ukraine of March 29, 2006 № 373, which approved the "Rules for ensuring the protection of information in information, telecommunications and information and telecommunications systems";[6]
- Order of the State Special Communications Administration dated 02.12.2014, № 660, which approved the "Procedure for assessing the security of state information resources in information, telecommunications and information and telecommunications systems"; the order was registered in the Ministry of Justice of Ukraine on January 28, 2015, for № 90/26535;[7]
- Order of the State Special Communications Administration dated 15.01.2016 № 20, which approved the "Procedure for scanning for vulnerabilities of state information resources posted on the Internet";[8]
- Decree of the Cabinet of Ministers of Ukraine of October 09, 2020, № 943, which approved the "Some issues of critical information infrastructure"; [9]

3 https://zakon.rada.gov.ua/laws/show/2163-19#Text
4 https://zakon.rada.gov.ua/laws/show/z0603-08#Text
5 https://zakon.rada.gov.ua/laws/show/1772-2002-%25D0%25BF#Text
6 https://zakon.rada.gov.ua/laws/show/373-2006-%25D0%25BF#Text
7 https://zakon.rada.gov.ua/laws/show/z0090-15#Text
8 https://zakon.rada.gov.ua/laws/show/z0196-16#Text
9 https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text

- Law of Ukraine “On Telecommunications”;[10]
- Law of Ukraine “On protection of information in information and telecommunication systems”;[11]
- Resolution of the Cabinet of Ministers of Ukraine dated 11.04.2012 № 295, which approved the “Rules for the provision and receipt of telecommunications services;[12]
- Resolution of the Cabinet of Ministers of Ukraine of April 12, 2002, № 522, which approved the “Procedure for connection to global data transmission networks”;[13]
- The Cyber Security Strategy of Ukraine approved by the Decree of the President of Ukraine on March 15, 2016.[14]
- Decree of Cabinet of Ministers of Ukraine, June 19, 2019 № 518, “On approval of the General requirements for cyber protection of critical infrastructure”[15]
- Decree of Cabinet of Ministers of Ukraine, October 9, 2020 № 1109, “Some critical infrastructure issues”[16]

NATIONAL CYBERSECURITY STRATEGY OF UKRAINE

The Cyber Security Strategy of Ukraine, approved by the Decree of the President of Ukraine on March 15, 2016, defines cybersecurity threats and respective priorities for ensuring the cybersecurity of Ukraine. This document is based on the provisions of the Council of Europe Convention on Cybercrime and aims to create conditions for the safe functioning of cyberspace and its use in the interests of individual, society and the state.[17] The Cyber Security Strategy of Ukraine (2016) was the first official document in the sphere of cybersecurity. It describes the main threats in the sphere of cybersecurity and recognizes “Cyberspace” as a separate (along with the traditional “Earth”, “Air”, “Sea” and “Space”) sphere of hostilities in which the relevant units of the armed forces of the world’s leading states are increasingly active. The strategy document describes the National cybersecurity system and regulates responsibilities for the main subjects of cybersecurity.

The second version of the National Security Strategy of Ukraine, approved by the Decree of the President of Ukraine on September 14, 2020, became the basis of many new strategies in different fields.[18] Security and development of cyberspace, introduction of e-governance, guarantee of security and sustainable functioning of electronic communications and national electronic information resources should be integral aspects of State policy on information space development and evolution of the Information Society in Ukraine. The strategy is based on three principles of state policy in the field of national security:

10 https://zakon.rada.gov.ua/laws/show/1280-15#Text
11 https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
12 https://zakon.rada.gov.ua/laws/show/295-2012-%25D0%25BF#Text
13 https://zakon.rada.gov.ua/laws/show/522-2002-%25D0%25BF#Text
14 https://zakon.rada.gov.ua/laws/show/n0003525-16#Text
15 https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
16 https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text
17 https://zakon.rada.gov.ua/laws/show/n0003525-16#Text
18 https://zakon.rada.gov.ua/laws/show/392/2020#n7

- Deterrence – development of security and defence capabilities to deter armed aggression against Ukraine;
- Resilience – the ability of society and the state to quickly adapt to changes in the security environment and maintain sustainable operation, in particular by minimizing external and internal vulnerabilities;
- Interaction – the development of strategic relations with key foreign partners, primarily with the European Union and NATO and their member states, the United States; and of pragmatic cooperation with other states and international organizations based on the national interests of Ukraine.

The Cybersecurity Strategy will aim in particular to: improve the security of network and information systems; introduce a risk management system; create conditions to provide resources including human cybersecurity; enhance operational and cybersecurity critical infrastructure; fight against cybercrime; use the capabilities of public-private partnership and interaction of stakeholders to address cybersecurity and cyber defence issues and increasing the level of online culture.

MAIN ACTORS IN CYBERSECURITY IN UKRAINE

The main authorities that ensure cybersecurity in Ukraine include the Ministry of Defence, the State Service of Special Communications and Information Protection (SSSCIP), the Security Service, the National Police, the National Bank, intelligence agencies, and the governmental CERT (CERT-UA) within the State Centre for Cyberdefence of the State Service for Special Communications and Information Protection of Ukraine.

The Ukrainian central government has established the national level cybersecurity coordination format for cybersecurity policy coordination. This format includes relevant public, private and third sector entities. The National Cybersecurity Coordination Centre is the working body of the National Security and Defence Council of Ukraine. The members of the Centre are:

- First Deputy or Deputy Minister of Defence of Ukraine
- Chief of the General Staff of the Armed Forces of Ukraine
- Head of the Security Service of Ukraine
- Head of the Foreign Intelligence Service of Ukraine
- Head of the National Police of Ukraine
- Head of the National Bank of Ukraine (with consent), whose responsibilities include cybersecurity issues
- Head of the Main Directorate of Intelligence of the Ministry of Defence of Ukraine
- Head of the Office of Intelligence of the Administration of the State Border Guard Service of Ukraine
- Head of the State Service for Special Communications and Information Protection of Ukraine

CERT-UA is the official government body that responds to computer emergencies of Ukraine, and operates within the State Centre for Cyberdefence of the State Service for Special Communications and Information Protection of Ukraine. Since 2009 CERT-UA

has been an accredited member of the FIRST Security Incident Response Team.[19] Tasks of CERT-UA include:

- Accumulation and analysis of data on cyber incidents, maintaining the state register of cyber incidents;
- Providing practical assistance to the owners of cybersecurity facilities on the prevention, detection and elimination of the consequences of cyber incidents on these facilities;
- Organization and holding of practical seminars on cybersecurity issues for the subjects of the national cybersecurity system and owners of cybersecurity facilities;
- Preparation of and posting on its official website recommendations for combating modern types of cyber-attacks and cyber threats;
- Interaction with law enforcement agencies ensuring their timely information about cyberattacks;
- Interaction with foreign and international organizations in response to cyber incidents, in particular in the framework of participation in the Forum of teams responding to security incidents FIRST with the payment of annual membership fees;
- Interaction with Ukrainian teams to respond to computer emergencies, as well as other enterprises, institutions and organizations, regardless of ownership, which carry out activities related to the security of cyberspace;
- Processing of information received from citizens about cyber incidents regarding cybersecurity objects;
- Assistance to state bodies, local self-government bodies, military formations formed in accordance with the law, enterprises, institutions and organizations regardless of the form of ownership, as well as to citizens of Ukraine in resolving issues of cyber defence and counteraction to cyber threats.

The Ministry of Defence of Ukraine and the General Staff of the Armed Forces of Ukraine in accordance with their competences are to be responsible for:

Implementation of the activities relating to the preparation of the State in repelling military aggression in cyberspace (cyber defence);

Development of military cooperation with NATO on issues of secure cyberspace and joint protection against cyber threats;

Provision of cyber protection of their own information infrastructure in cooperation with the State Service of Special Communications and Information Protection of Ukraine and the Security Service of Ukraine.

The State Service of Special Communications and Information Protection of Ukraine is to be responsible for:

- Formation and implementation of the national policy on protection of state information resources in cyberspace and information security, since the requirement of information protection was imposed by the law, cyber protection of critical information infrastructure and the required state control in these spheres;
- Coordination of cyber defence activities of other cybersecurity entities;

[19] https://www.first.org/members/teams/cert-ua

- Implementation of organizational and technical measures to prevent, detect and respond to cyber-attacks and cyber incidents; mitigate any effects of them, inform about cyber threats and relevant methods of protection against them;
- Support of the State Cyber Centre;
- Security audit for identifying vulnerability of critical information infrastructure.

The Security Service of Ukraine is to be responsible for:

- Prevention, detection, suppression and exposure of crimes against the peace and security of mankind committed in cyberspace;
- Implementation of counterintelligence and operational-investigative measures to combat cyber-terrorism and cyber espionage, as well as assure readiness of critical infrastructure to deal with possible cyber-attacks and cyber incidents;
- Cybercrime prevention, the potential impacts of which directly pose a threat to the vital interests of Ukraine;
- Investigation of cyber incidents and cyber-attacks on national electronic information resources, critical information infrastructure, information, since the requirement of information protection is imposed by the law;
- Computer emergency response (CERT) for national security.

The National Police of Ukraine are to be responsible for:

- Protection of human and civil rights and freedoms, defence of society and state interests from criminal attacks in cyberspace;
- Prevention, detection, suppression and exposure of cybercrime;
- Raising public awareness about security in cyberspace.

The National Bank of Ukraine is to be responsible for establishing requirements for cyber protection of critical information infrastructure in the banking sector.

Intelligence agencies of Ukraine are to be responsible for conducting intelligence activities to identify threats to Ukraine's national security in cyberspace, and intelligence-gathering operations aimed at other events and circumstances relating to cybersecurity matters.

The Ukrainian Parliament Commissioner for Human Rights carries out personal data protection.

PROTECTION OF CRITICAL CYBERSECURITY INFRASTRUCTURE (INFORMATION)

Ukraine still lacks a nationwide systematic approach that encapsulates management, protection and security of the whole aggregate of such systems, including objects and resources, considering that mutual interface exists between some objects customarily attributed to critical infrastructure. Furthermore, there is still no mechanism to prevent potential crisis situations associated with CI operation. Implementation of such a mechanism would require a profound survey of existing practices for critical infrastructure protection (CIP) in Ukraine, which are currently dominated by departmental approaches. There is inadequate interaction and coordination between appropriate government agencies for analysing data, and ways and practices in the enhancement of security and

resilience of critical infrastructure also fall short. The primary concern of cyber protection of critical infrastructure in Ukraine consists of:

- Integrated improvement of legal framework for cyber protection of critical infrastructure;
- Definition of criteria for classification of automated information systems, telecommunications systems, information and telecommunication systems as critical information infrastructure;
- Establishment and operations support of the public register of critical information infrastructure;
- Regulation of requirements to cyber protection of critical infrastructure;
- Establishment and operations support of cyber defence units by the owners (despondent owners) of critical infrastructure;
- Determination of qualification criteria for certain categories of employees of critical infrastructure with account of current trends in cybersecurity and urgent cyber threats; introduction of mandatory periodic performance appraisal of employees for compliance with specified criteria;
- Establishing cooperation among cybersecurity entities which provide cyber protection of critical infrastructure; development of public-private partnership on cyber threats prevention; response to cyber-attacks and cyber incidents, elimination of their negative effects, particularly in the cases of crisis situations, special contingency period, state of emergency and martial law;
- Development and application of the scheme for information exchange among the state agencies, private sector and citizens regarding the threats to critical information infrastructure.

As for the spectrum of 'Critical Infrastructure' threats existing in Ukraine, their nature is shaped by the security environment currently faced by the country. Hostilities as part of the Anti-Terrorist Operation in the Donbas Region, featuring high level of wear of capital assets and serious problems with environmental and anthropogenic safety, rapidly increases the level of threat of accidents at high hazard assets such as coal mines, power sector facilities, chemical factories and steelworks, as well as in the utility networks - whether as the result of incidental damage, loss of process control, or as a consequence of terrorist acts of sabotage.

The existing Ukrainian legal framework governing issues allied to CIP classifies emergencies, rather than threats, based on their origin. Article 5 of the Civil Protection Code of Ukraine specifies that, depending on the origin of events that may cause emergency situations in Ukraine, the following types of emergency situations could be distinguished: 1) man-induced; 2) natural; 3) social; 4) military.

NATIONAL AND INTERNATIONAL CYBERSECURITY COOPERATION

In recognizing the need for greater and stronger international cooperation and capacity building to address cybersecurity, the needs and threats that arise are also highlighted in the new Cybersecurity Strategy of Ukraine. Ukraine has been collaborating with a number of partners across the cyber domain. Ukraine has been a partner in the joint

European Union and Council of Europe projects "Cybersecurity EAST"[20], which have a regional dimension involving all countries of the Eastern Partnership (i.e., Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova, Ukraine). The Ukrainian engagement with the ISPs and the Council of Europe recommendations are already benefitting the national authorities as they have fostered a structured dialogue with ISPs that has served as a trust-building exercise towards understanding and responding to each other's needs.

In the cyber defence field, Ukraine is working with the NATO Cyber Defence Trust Fund[21] to enhance the country's technical capabilities in countering cyber threats. In addition, Ukraine became the top beneficiary of Science for Peace and Security (SPS) Programme of Cooperation. NATO allocated 2.2 million EUR for SPS cooperation with Ukraine in 2014 contributing to a projected total of 10 million EUR in 2014-2017.[22] Assistance includes establishing an Incident Management Centre (IMC) to monitor cybersecurity events, as well as laboratories to investigate cybersecurity incidents, coupled with training in employing this technology and equipment. The Security Service of Ukraine is taking the lead role in the framework of the Trust Fund, with the NATO partner Romania as the lead nation, with additional financial and in-kind contributions from Albania, Estonia, Hungary, Italy, Portugal, Turkey, and the United States. Together with the NATO partners, Ukraine has conducted cyber defence exercises and trainings where all the relevant national stakeholders are trained on how to react to major cyber-attacks at the national defence infrastructure.

Ukraine is not only participating in international initiatives in the sphere of countering cyber threats but also contributing to the development of regional initiatives. A Ukraine-led initiative established a working group on cybersecurity in the framework of the GUAM Organization for Democracy and Economic Development (i.e., Azerbaijan, Georgia, Moldova, Ukraine). The group is now discussing the development of a Memorandum of Understanding (MoU) for adoption by its governments, while it has already put in place a protected communication system which allows, inter alia, the secure exchange data online and conducting of video conferences.[23]

CONCLUSIONS

Ukraine already had some framework in place related to the field of cybersecurity; however, growing and evolving challenges are calling for a fast and comprehensive revision and improvement of the technical and operational sides of cybersecurity (legal framework, key stakeholders, cooperation mechanisms, technical set-up). In early 2016, the government approved the first Cybersecurity Strategy of Ukraine, with the objective of "creating conditions for the safe functioning of cyberspace, application of cyberspace to benefit individual, society and the State". At the moment, the second version (the 2020 strategy), currently in its draft stage, is looking to address and improve upon the issues of communication and coordination between the governmental agencies.

Ukraine lacks financial incentives to attract the best specialists to work for the government, and there is a sizable problem of cooperation between the public and private sectors, which is crucial for success in cybersecurity. Cyber is one of the fields that clear-

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

21 https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160712_1606-trust-fund-ukr-cyberdef.pdf

22 https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2015_12/20151130_1512-factsheet-nato-ukraine-supportr_en.pdf

23 https://thegfce.org/cybersecurity-in-ukraine-national-strategy-and-international-cooperation/

ly demonstrates the interdependence of Ukraine. Much of the enhancement of the Ukrainian cyber defence would have not been possible without the financial and training help of the Western partners. In order to achieve strong cybersecurity in the country, Ukraine should ensure the same range of development between ICT sector and cybersecurity infrastructure. Unfortunately, the area of public-private partnership is in an early stage of development.

To achieve a better cybersecurity at the national level, Ukraine has to work on:

- Building capacity in military cyber defence;
- Developing a cyber-crisis management plan;
- Developing its operational centres and essential e-services and CII operators;
- Promoting cybersecurity education through curricula for primary, secondary and vocational education as well as through media campaign nationwide (TV, radio, newspapers, etc.).

All the actions mentioned need large amounts of resources. For instance, in cyber defence there is a need for technical laboratories to develop skills and knowledge as well as national and international expertise in cybersecurity and cyber defence capable of teaching new professionals in the cyber field. For developing operational centres, the need for specialists, hardware and software support, regular cybersecurity training and exercises is required to implement the best strategies and plans at developing a strong e-service in the country. In addition, for media campaigns and curricula there will be needed qualified cyber and IT professionals together with the academic environment to ensure a working group that will implement all the necessary information for a well-educated society in cybersecurity.

It will cost a lot of effort but it is worth the cause, as cyber threats are rising annually in Ukraine, and the Ukrainian society has been exposed to the risk of cyber-attacks many times in the last decade.

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