DCAF Geneva Centre
for Security Sector
Governance

Moldova 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 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 in universities to prepare a qualified workforce for the cybersecurity sector of Moldova, and others. She holds in responsibility for strategic planning and international and intergovernmental cooperation, national cybersecurity policy, international coordination with MFA, and international projects on various tasks related to cybersecurity.

As a cybersecurity expert, Ms. Spinu 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, Moldova, national strategy, 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 report presents the main cybersecurity threats in Moldova and the needs arising from national security objectives. After analysing the national cybersecurity strategy for Moldova, an identification and need for the main actors within the state who would be responsible for the implementation of the national strategy on cybersecurity was undertaken. A national action plan for cybersecurity was designed. It was understood that for a responsible and developed society there is a necessity to collaborate with the private sector and academia, and thus a robust cooperation and communication mechanism was described to include all the relevant stakeholders. The report reflects the conclusions and final remarks that have made the operational cybersecurity architecture in Moldova an elaborate framework.

Purpose of this Report

This report has been made to present and generate brief but detailed background information on the situation in cybersecurity governance and management point of view with the aim of identifying future reform needs for the purposes of long-term and needs-based reform objectives for cybersecurity capacity building.

Although there are a multitude of aspects relevant to cybersecurity capacity building, due to the open nature of this report and the information available, we limit our analysis to the normative framework and the main actors of the cybersecurity sector. Given the scarcity of information regarding some of these areas, the space devoted to each in the report varies.

Preface

The Republic of Moldova, as an integral part of the European space, is going through a process of transition to an information society. According to the provisions of the Association Agreement between the Republic of Moldova, the European Union and the European Atomic Energy Community and their Member States, priorities are set to encourage and promote the implementation of information technology tools and communications (ICT) for better governance, e-learning and research, public health care services, digitization of cultural heritage, development of digital content and e-commerce, as well as personal data and the protection of confidentiality in electronic communications.

Main cybersecurity threats and needs in Moldova

Each country faces its own unique set of cybersecurity challenges; its capacity to respond to these challenges varies, so do the tools at its disposal. The concern is not so much with cyber war or the online vulnerability of national infrastructure but with issues such as censorship, warrantless surveillance of email traffic or the gathering and retention of private data by IT firms. The political, economic, social and military fields are targets of the information war that tends, in particular, to influence decision-making processes. For Moldova, the critical infrastructure remains its essential services, with networks linked to its regional partners, governmental institutions, and security services. As Moldova strives to take on the road to digitalisation, more and more essential services get online and are critical in nature.

The following is a loosely stated definition of cybersecurity: Security in cyberspace (i.e., cybersecurity) is about technologies, processes, and policies that help to prevent and/or reduce the negative impact of events in cyberspace which can happen as the result of deliberate actions against information technology by a hostile or malevolent actor. To go beyond this loosely stated definition of cybersecurity, it is necessary to elaborate on the meaning of "impact," on what makes impact "negative," and on what makes an actor "hostile" or "malevolent".

The globality of cyberspace is likely to amplify risks to the public and private sector equally. Threats to cyberspace can be classified in several ways, but the most common are those based on motivational factors and those that impact the society. In this sense, we can consider cybercrime, cyber terrorism, and cyber warfare, having at its source both state and non-state actors.

In Moldova, the specific objectives of the action plan of the National Cybersecurity Strategy reflect the needs and threats existing at that stage in the country. The adjustment of the legal framework and the delegation of the main state actors to implement measures according to their competences have resulted in the development of a community responsible for cybersecurity. The Republic of Moldova tries to adapt its policy and strategy to the best models and examples in the region, and in accordance with international directives such as EU Directive 2016/1148[1], Regulation (EU) No 526/2013, NIS Directive, Directive 2009/140 / EC, Directive 2002/21 / EC.

According to the data of the Special Telecommunications Centre (now CERT Gov within ITSEC), the number of cyber-attacks on web servers increased from 2013 to 2014 by about 26%, and the vulnerabilities of open ports increased by about 385%. The chances of infecting computers with computer viruses have increased by about 27%. The number of incidents on government e-mail decreased in 2014 compared to 2013 by about 1%. At the same time, the share of these incidents in the total number of cyber-attacks has decreased. In 2014 this share was decreased to 40%, compared to 51% in 2013. Based on the analysis, the basic problem identified was the lack of a cybersecurity management system, to carry out coordinated planning and efficient use of available resources, and to identify vulnerabilities and risks following the audit of cybersecurity, as well as the interventions necessary to diminish the harmful impact of crime, cyber-attacks and incidents on the secure development of public information. This system is required to be extended to all spheres of social, economic and socio-political life. It must be created and implemented by the targeted public and private domain entities.

Cyber fraud, cyber-attacks, electronic payment fraud and child pornography on the global Internet are types of crimes requiring specialized investigations, proper training and endowment of law enforcement agencies. Cybercrime is a criminal phenomenon that in turn fuels many risks and crises in cyberspace; preventing and combating cybercrime must be a major concern for all actors involved, especially at the institutional level, where the responsibility for developing and implementing coherent policies in the field lies. Threats and risks, cyber-attacks and incidents, as well as other events occurring in the cyberspace are materialized through the exploitation of human, technical and procedural vulnerabilities. In recent years in the Republic of Moldova, there has been an increase in indicators on the number of cybercrimes linked to computer systems and the number of cyber-attacks on information resources published on the Internet. Many applications and their vulnerabilities are being exploited for theft, modification, and deletion of information. The main problems concerning governance at the national level are:

- The lack of complex audits on cybersecurity. There are no studies or reports reflecting in detail the situation regarding cybercrime[2] (cyber risks and threats, cyber-attacks and incidents, other events that occurred in the cyberspace), the number of victims and the amount of related economic damage;
- The lack of a national CERT (Cyber Security Incident Response Centre), an entity responsible for the prevention and the response to cybersecurity incidents;
- The lack of an integrated cybersecurity management system, to plan and coordinate the use of available resources, to identify vulnerabilities and risks following a cybersecurity audit, as well as the interventions needed to mitigate the harmful impact of crime, attacks and cyber incidents on the secure development of the information society;
- The lack of an integrated cybersecurity management system at the national level also means that complete, true, up-to-date and structured data is missing, which in turn creates obstacles in identifying optimal solutions;
- The insufficiency of qualified specialists in the field of information technologies and the low level of salaries, especially in the public sector;
- Some state and non-state actors exploit the lack of an international legal framework in areas such as cybersecurity, the lack of responsibility for regulating digital media, and take advantage of any ambiguity in these matters;
- The lack of specialized training programs for employees with criminal investigation and prosecution responsibilities, prosecutors, judges, specialists and judicial experts in the field within law enforcement structures, as well as trainings addressed to technical staff in public institutions in the field of cybersecurity;

[2] The only official sources of statistical data on cybercrime are the Register of Crimes, Criminal Cases, Criminals and Crime Materials, held by the Ministry of Internal Affairs and the Automated Information System, Criminal Investigation: E-dosar, managed by the General Prosecutor's Office.

- Insufficient specialized equipment and software for investigating computer crimes;
- Reduced funding for the participation of specialists in international capacity building projects and events, and the exchange of good practices.

Solving specific problems requires interventions in the legislative, institutional, normative and technical-normative frameworks. There is a need for continuous training and certification of cybersecurity specialists, and for cybersecurity auditing of entities that own cyber infrastructures, information systems and communication networks, including those providing computer and electronic communications services.

Cyber-attacks mainly target state infrastructures due to the sensitive information they attempt to obtain. In 2015, the National Bank of Moldova was a victim of a DDos cyber-attack which blocked access to NBM data available on the Internet.[3] As a result, the official NBM website was temporarily unavailable. There were no data losses or corruptions managed by the NBM. In 2017, an estimated six million cyberattacks took place in Moldova. The targets of hackers were both state institutions and private companies, and cyber vulnerabilities remained on the agenda this year. One of the most resounding cyber-attacks was WannaCry, which affected more than 90 countries including 40 users in the Republic of Moldova[4]. In May 2020, the Ministry of Internal Affairs of Moldova and the Directorate for the Investigation of Organized Crime and Terrorism of Romania had reasonable suspicion over a case at the beginning of 2020; an organized criminal group was formed consisting of four people operating in the virtual environment under the title "Pentaguard", with the aim of committing crimes specific to cybercrime. According to the institution, through this type of attack there is a risk of blocking and seriously disrupting the functioning of the IT infrastructures of hospitals and part of the health system playing at the time a decisive role in combating the new Coronavirus pandemic[5].

Elections are another popular target in the country; during both the parliamentary elections in 2019 and the presidential elections in 2020, cyber-attack attempts have been identified. During the 2019 parliamentary elections, the Information Technology and Cyber Security Service was responsible for hosting the official pages of the Central Electoral Commission and for the maintenance of over 4200 secure channels between polling stations in the Republic of Moldova – including 300 secure channels for polling stations, voting from outside the country – and other government infrastructures that contained information on the conduct of parliamentary elections and preliminary results.

According to a detailed report by the ITSEC on the cybersecurity incidents recorded during the 2019 parliamentary elections, initiated both inside and outside the country, several attempts were made to render the information technology infrastructure unavailable, including attacks on electronic communications from the Central Electoral Commission as well as attempts to gain unauthorized access to the components involved in securing the parliamentary election infrastructure, in order to make change to the accessed electronic content. By applying special prevention and response measures according to the type of attack and its specificities, the specialists of the Information Technology and Cyber Security Service could react promptly to all identified threats and deviations, and managed to block cyber-attacks in time to ensure the proper functioning of the system, allowing the results of the parliamentary elections of February 24 to be presented in a

[3] https://www.zdg.md/stiri/stiri-economice/atac-cibernetic-asupra-resurselor-informatice-ale-bnm/

[4] https://primelestiri.md/republica-moldova-lovita-de-atacurile-cibernetice-tintele-hackerilor-au-fost-atat-institutiile-de-stat-cat-si-cele-private---64101.html

[5] https://www.jurnal.md/ro/news/95281788303fe863/o-grupare-de-hackeri-pregatea-atacuri-cibernetice-asupra-unor-spitale-din-romania-liderul-e-din-republica-moldova.html

transparent and protected form[6]. During the 2020 presidential election, internal protection and anti-corruption specialists identified a cyber-attack manifesting through abusive calls from several telephone numbers. The purpose of the cyber-attack was to block the network of subscribers, including officials of the Ministry of Internal Affairs[7].

At the current stage, propaganda, misinformation and/or manipulative information are extremely dynamic, and the resources allocated for this purpose by third parties far exceed the response and combat capabilities of the Republic of Moldova. Government, public administration authorities, institutions and enterprises state that regardless of the form of organization, civil society has established the following strategic vision: "The Republic of Moldova will ensure a secure information space for all subjects of law by harmonizing the legal framework and its implementation, thus protecting fundamental human rights and freedoms and promoting democracy and the rule of law". To achieve this strategic vision, general objectives, implementation, actions and progress indicators have been articulated in an act called the National Cyber Security Strategy (2016-2020).

Laws and normative acts on cybersecurity in Moldova

The issue of cybersecurity and the first measures for solution at the level of government policies are explored for the first time in the National Strategy for the development of the information society "Digital Moldova 2020", approved by Government Decision no. 857 of 31.10.2013. At the same time, this issue was examined at meetings of the Supreme Security Council, during which a series of recommendations was formulated, and approved by Supreme Security Council Decision no. 01/1-02-05 of 07.10.2014.

In the context of implementing the provisions of these two legal acts, the elaboration of the National Cyber Security Program of the Republic of Moldova for the years 2016-2020 was initiated, approved by Government Decision no. 811 of 29.10.2015[8]. The main objective of the plan is "Creating and implementing a cybersecurity management system of the Republic of Moldova, with the process of implementing information technologies in all areas of life (economic, social, etc.) in the country".

Simultaneously, when carrying out the actions for 2016-2020, the provisions related to cybersecurity set out in the Information Security Strategy of the Republic of Moldova for 2019-2024 (ISS 2019-2024) were approved by Parliament Decision no. 257/2018[9]. The National Defense Strategy for the years 2018–2022 (NDS 2018-2022) was approved by Parliament Decision no. 134/2018[10], and the National Security Strategy approved by Parliament Decision no. 153 of 15.07.2011[11]. According to the provisions of the Government Decision no. 811 of 29.10.2015, the Ministry of Economy and Infrastructure (MEI) is responsible for monitoring and coordinating the process of achieving the PNSC 2016-2020.

To ensure the adjustment of the normative-legislative framework on cybersecurity of the Republic of Moldova, it will provide: a) a definition of terms (notions) in the field of cybersecurity; b) a delimitation by fields of competencies; c) the establishment of a

[6] https://stisc.gov.md/ro/incidentele-de-securitate-cibernetica-inregistrate-perioada-alegerilor-parlamentare-2019-au-fost

[7] https://www.mai.gov.md/index.php/ro/news_anticoruption/atac-cibernetic-adresa-functionarilor-mai

[8] https://www.legis.md/cautare/getResults?doc_id=101028&lang=ro

[9] https://www.legis.md/cautare/getResults?doc_id=111979&lang=ru

[10] https://www.legis.md/cautare/getResults?doc_id=110013&lang=ro

[11] https://www.legis.md/cautare/getResults?doc_id=105346&lang=ro

body with monitoring functions for the observance of the cybersecurity requirements; d) the designation of a body responsible for controlling the implementation of the cybersecurity audit results; e) the obligations of the holders of state information systems towards the periodic performance of these systems' audit, with the establishment of the periodicity, levels, and obligations to present reports to the competent body; f) sanctions for non-compliance with the audit decision regarding the mandatory minimum requirements for cybersecurity; g) the personal responsibility for ensuring cybersecurity; h) the introduction in public authorities of the function of a cybersecurity coordinator, including its main attributions; i) the formation of the Cybersecurity Intersectoral Council (with the function of coordinating cybersecurity activities), which was elaborated and approved by Government Decision no. 201/2017[12] regarding the approval of the Mandatory Minimum Cyber Security Requirements. To establish an institution responsible for conducting the audit and assessing its compliance, Government Decision no .414/2018[13] was developed and measures to strengthen data centres in the public sector and streamline the administration of state information systems were approved. In addition, this Decision provides for the designation of public institutions: the Information Technology and Cyber Security Service (ITSEC) and the Electronic Government Agency (E-governance) with new responsibilities in the field of cyber security. At the same time, the Concept of Information Security of the Republic of Moldova was developed and approved by Law no. 299 of 21.12.2017[14]. In accordance with art. 3 of the Concept of Information Security, the Information and Security Service (ISS) was developed and finalized jointly with the competent national authorities in the draft Information Security Strategy of the Republic of Moldova for 2019-2024, as well as the Action Plan for its implementation, subsequently approved by Parliament Decision no. 257 of 22.11.2018[15].

In order to achieve Parliament Decision 257/2018, the SIS initiated a procedure for creating a Coordinating Council for ensuring information security, which will have certain responsibilities in the field of cybersecurity. In this regard, the SIS drafted and submitted to the competent institutions/organizations the Government Decision draft "On the creation of the Coordinating Council for ensuring information security". Subsequently, working meetings were held with government institutions, private ICT companies (represented by Moldova IT Park and ATIC), representatives of civil society and media institutions. After receiving all the suggestions of the institutions/organizations involved, the SIS will finalize and submit the Government Decision draft for promotion.

In the same vein, the MEI has initiated the procedure for drafting the law transposing EU Directive 2016/1148 concerning measures for a common high level of security of networks and information systems across the Union. Best practices in the field of network and information systems security are currently being examined for inclusion in the project. By the MEI Order no. 54 of 04.03.2019, a working group for the elaboration of the draft law on the security of networks and information systems was created.

In 2016, for the harmonization of electronic communications legislation with relevant EU framework directives, the MEI drafted a law for amending and supplementing the Law on electronic communications no. 241-XVI of 15.11.2007[16], based on the provisions of the EU framework directives in the field of electronic communications, provided in the Association Agreement "Republic of Moldova - European Union". The draft proposes to supplement the Law in question with two new articles (art. 201 and art. 202), which refer

[12] https://www.legis.md/cautare/getResults?doc_id=98644&lang=ro
[13] https://www.legis.md/cautare/getResults?doc_id=124094&lang=ro#
[14] https://www.legis.md/cautare/getResults?doc_id=105660&lang=ro
[15] https://www.legis.md/cautare/getResults?doc_id=111979&lang=ro
[16] https://www.legis.md/cautare/getResults?doc_id=112412&lang=ro#

to the security and integrity of networks and services. Through these additions, national legislation has been harmonized with the provisions of Chapter III-A, "Security and integrity of networks and services" of Directive 2002/21 / EC, as amended by Directive 2009/140 / EC[17].

The draft law in question was approved by Law no. 185 of 21.09.2017[18] for the amendment and completion of some legislative acts. After the republishing of the Law on electronic communications no. 241-XVI of 15.11.2007 in the Official Gazette of the Republic of Moldova no. 399-410 of 17.11.2017, art.679, the respective provisions can be found in art. 21 and art. 22 of this law. ISS, as a partner institution, shall, within the limits of its competences, provide the necessary support to the relevant institutions. In this context, the Regulation on the application of the electronic signature on electronic documents by the officials of legal entities under public law within their electronic circulation was approved, by Government Decision no. 1141 of 20.12.2017[19], as well as the Regulation on the activity of providers of certification services in the field of electronic signature application, by Government Decision no. 1140 of 20.12.2017.

In accordance with the provisions of the Information Security Strategy of the Republic of Moldova 2019-2024 (PD 257/2018), Government Decision no. 482 of 08.07.2020[20] "On the approval of necessary measures on ensuring cybersecurity at government level and amending Government Decision no. 414/2018 on measures to consolidate data centres in the public sector and to rationalize the administration of state information systems", I.P. ITSEC is designated as the Governmental Cyber Security Incident Response Centre (CERT-Gov). CERT-Gov is the single point of contact and reporting of cybersecurity incidents for departmental CERT-type structures and has the necessary capacity to prevent, analyse, identify and respond to cyber incidents at the governmental level. In this context, GD 482/2020 delimits the competencies and responsibilities of public entities in the field of cybersecurity, including the measures and mechanisms necessary for implementation and maintaining a secure cyberspace at government level.

For preventing and combating computer crime, Law no. 294 of 22.12.2016 was developed and adopted for the completion of article 118 of the Code of Criminal Procedure of the Republic of Moldova no. 122-XV of March 14, 2003. The purpose of approving the proposed amendments is to carry out an examination, by the prosecuting authority, of computer systems or computer data storage media with the consent and in the presence of the person owning or controlling these objects, which would give a clearer explanation for the accumulation of evidence and their presentation in court.

Adjustments to national legislation on the provisions of the Council of Europe Convention for the Protection of Children against Sexual Exploitation and Sexual Abuse and the Additional Protocol to the Convention (Lanzarote, 25 October 2007) were also made in the Ministry of Foreign Affairs and European Integration request of 09.01.2020. The Ministry of Internal Affairs positively endorsed the draft normative act elaborated in 2018 which regulates the national mechanism for monitoring and reporting the implementation of the Lanzarote Convention.

[17] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF

[18] https://www.legis.md/cautare/getResults?doc_id=101154&lang=ro

[19] https://www.legis.md/cautare/getResults?doc_id=102490&lang=ro

[20] https://www.legis.md/cautare/getResults?doc_id=102490&lang=ro

National Cybersecurity Strategy of Moldova

Over the last decade, the Republic of Moldova has developed several country strategies, programs and policies for the development of the information society at national level, in accordance with the recommendations of European and international forums in the field of information technology and electronic communications- in both online and offline environments. The first cybersecurity strategy was adopted by Government Decision no. 811 of 29.10.2015, and the Ministry of Information and Communication Technology was established for monitoring and coordinating the implementation of the National Cyber Security Program. In the first strategy, the main concept of cybersecurity in the country and its principals were established: protection of fundamental human rights and freedoms; access for all; cyber resilience; multi-participative administration; shared responsibility and personalized responsibility for ensuring cyber security.

The estimated costs for obtaining the expected results, totalled on the shares within each objective of the Program for 2016-2020, were as follows:

1. Secure processing, storage and access of data, including data of interest public – 9 504 000 MDL;
2. Security and integrity of electronic communications networks and services – 1 944 000 MDL;
3. Development of prevention and urgent response capacities (CERT network national) – 49 608 000 MDL;
4. Preventing and combating cybercrime - 2 916 000 MDL;
5. Consolidation of cyber defence capacities – 2 232 000 MDL;
6. Education, training and continuous information in cybersecurity – approx. 10 089 000 MDL;
7. International cooperation and interaction in the spheres related to cybersecurity - 648 000 MDL.

The preliminary estimated cost for full implementation of the Program is of 76 941 000 MDL (approx. 3.655.380,14 Euro). The expected result of the Program implementation is a security management system of the Republic of Moldova, created and implemented in the targeted entities in the public and private domains, that will ensure the planning and use of available resources, and the identification of interventions needed to mitigate the harmful impact of crime, attacks and cyber incidents on the secure development of the information society. This system is to be extended to all spheres of social, economic and political life in the country. The purpose of the National Cyber Security Strategy is to legally correlate and systemically integrate priority areas with responsibilities and competencies to ensure information security at the national level based on cyber resilience, multimedia pluralism and institutional convergence in security – and aims to protect the sovereignty, independence and territorial integrity of the Republic of Moldova.

The Final Implementation Evaluation Report will be prepared at the end of 2020. The program will reflect the achievement of its objectives and the execution of the actions provided in the Action Plan, including the impact of the implementation of the Program on security cybernetics of the Republic of Moldova. The final report will include conclusions and proposals on the development and extension of implementation results in other spheres of social, economic and policies in the country. After the results were collected in the last period of the evaluation plan on National Cybersecurity Strategy

2016-2020, the Informational Security Strategy of the Republic of Moldova was created for 2019-2024. The current complex of actions is divided into four pillars:

1. Ensuring the security of the information-cyberspace and cybercrime investigation;
2. Ensuring the security of the information-media space;
3. Operational capacity building;
4. Streamlining internal coordination and cooperation processes in the field of information security.

The strategy incorporates some fundamental requirements to achieve a better cybersecurity governance at the national level, as well as a list with proposed actions and performance indicators.

National Informational Security Strategy 2019-2024

General goals, actions and progress indicators were established for an efficient implementation of the national cybersecurity strategy for the period of 2019-2024. The cybersecurity strategy brings to the table some main directions of action to establish a stronger cyber defence at the national level.

1. It is proposed to create an effective legal framework that will ensure state security in terms of each component, reduce risks, threats or even exclusion, create or designate a national CERT entity, and elaborate mechanisms for the creation and consolidation of departmental response centres to cyber and information security incidents in both public and private jurisdictions.
2. The problems facing the Republic of Moldova are highlighted by an increase in the number of cybercrime and contraventions, the number of cyber-attacks on information resources published on the global Internet, and by the shortage of competent human resources. It is proposed to initiate amendments to the main legislative acts (such as Government Decision no. 986 of 24 December 2012) to prevent and combat cybercrime in order to harmonize legislation in this field and develop sectoral programs dedicated to employees with powers of investigation and prosecution.
3. Media space: misinformation, propaganda and manipulative information from the outside are part of the basic problems. As improvement solutions established in Pillar II, it is proposed to develop and adjust functional legal mechanisms to counteract the phenomenon of misinformation and/or manipulative information that directly endanger the security of the information space.
4. The counter-intelligence and security component defines the issues around large-scale expansion by various actors in the use of means of interference in internal relations through propaganda and media aggression, as well as informational-psychological influence, in order to destabilize socio-political equilibrium and undermine the sovereignty and territorial integrity of the Republic of Moldova. Simultaneously, active information campaigns carried out by international terrorist organizations are designed to undermine and increase the level of hatred against the rule of law and values universally accepted by the international community.
5. The importance of raising awareness and educating society on such values is one of the prerogatives set out in the Strategy, which is to be developed and publicized in perspective. Currently, there is a lack of capacity to protect against the phenom-

enon of defamation on online platforms, which affects the exercise of human rights and fundamental freedoms. It also highlights the importance of awareness, education, media and cyber competence in the Republic of Moldova to allow citizens to critically analyse media content in order to identify propaganda.

In this sense, the authors of the Strategy propose actions to be taken in the direction of ameliorating the problems in this compartment through actions outlined in Pillars II and IV. The prerogative of harmonizing the regulatory framework and the elaboration of communication policies between state authorities and civil society would allow the consolidation of all legal subjects in a consultative and decision-making process. As a result, it will increase the degree of trust in the actions of state authorities in the context of defending the fundamental rights and freedoms of citizens, and will allow them to be aware of the need to adopt civic behaviour. To ensure a strong cybersecurity in Moldova, we need to invest resources in many segments:

- Harmonizing the legislative framework with European and International requirements and tendencies on cybersecurity;
- Professional training in the field and realization of some actions of awareness and understanding at the level of the decisional factors within public organizations;
- Improving both national and international collaborations in order to mitigate risks;
- Setting balance and boundaries between privacy and security;
- Ensuring and developing security by design for governmental and national services;
- Establishing a national CERT and ensuring mobile groups for incident response;
- Increased focus on opening up communication channels, setting up working groups and public consultation, involving civil society and public-private partnerships.

Main actors in cybersecurity in the country

In the general context of cybersecurity discussions, at the national level it is important to conceptually separate the main directions of action: cyber defence, cybercrime, national security, critical infrastructure and emergencies, international cyber diplomacy, and Internet governance. Cyberspace-specific threats are characterized by asymmetry, accentuated dynamics and global character, which makes them difficult to identify and counteract with measures proportional to the impact of the materialization of risks. In order to divide the responsibilities related to the national cybersecurity strategy, the Republic of Moldova relies on the organization of a state structure depending on the security directions mentioned above. As such, there are many actors in the national structures having to manage different cyber threats. Several actors are ensuring a high level of national cybersecurity against different types of cyber-attacks:

Security and Intelligence Service (SIS) of the Republic of Moldova

Established in 1999 by the Law of the Republic of Moldova no. 676-XIV and the reorganization of the Ministry of National Security into the Security and Intelligence Service (SIS) of Moldova, the SIS is a body specialized in state security. In 2010, through the RM Governmental Decision no. 84 on the transfer of state enterprise, the Centre for Special Telecommunications (CST) passed from the management of Security and Intelligence Service of the Republic of Moldova to the management of the State Chancellery (the CTS was created in subordination of SIS on 11 June 2002 - through the Government of the Republic of Moldova no. 735 on special telecommunication systems of Moldova - to protect important information of the state, create, manage and ensure the operation and development of special national telecommunication systems).

Its mission is to ensure an efficient protection of fundamental rights and freedoms of citizens, society and state against risks and threats to state security, promote democratic values and the national interests of the Republic of Moldova.

P.I. Information Technology and Cyber Security Service

The areas of competence of the Service are:

- Management of the information technology infrastructure and the Telecommunications System of the public administration authorities as part of the special communications network;
- Administration and maintenance of state information systems;
- Cyber security;
- Management of the unique public key infrastructure (PKI) of the Government;
- Implementation of information technologies in the public sector.

The organization hosts the governmental computer security incident response team "Centre for Response on Cybersecurity Incidents CERT-GOV-MD" as an internal subdivision, responsible for the implementation of Government Decision no. 482 of 08-07 -2020 on the approval of necessary measures to ensure cybersecurity at the governmental level, the amendment of Government Decision no. 414 of 08-05-2018 on security measures consolidation of data centres in the public sector, and the streamlining of the administration of state information systems based on Order no.56 of 10-06-2020 by the Director P.I. ITSEC.

E-Governance Agency

In 2010 the Moldovan Government engaged in an e-transformation process to streamline governance through intensive use of information technology. For this purpose, the State Chancellery established in August 2010 the public entity e-Government Centre – a team of professionals with an innovative and systemic approach towards the modernization of public services – to bring the Government closer to the Moldovan citizens. Since 2011 the Moldova e-Governance Agency has successfully implemented more than 100 products within more than 20 initiatives, having built a sustainable platform for further modernization of public services and other governance-related innovations. The beneficiaries of e-governance products are the citizens and visitors of the Republic of Moldova, the private sector and public institutions.

Ministry of Internal Affairs

The Ministry of Internal Affairs of the Republic of Moldova[21] has several subordinate institutions such as the General Inspectorate of Police and the Technology Service; various cybersecurity incidents are handled depending on their complexity and vectors of cybersecurity threats. The Centre for Combating Cyber Crimes (CCCC) of the National

[21] https://www.mai.gov.md/

Investigation Inspectorate, within the General Inspectorate of Police in the Ministry of Internal Affairs, was founded on 5 March 2013 after the reform of the MIA, according to the Government Decision no. 986 of 24 December 2012. It is a subdivision which performs investigative activity, especially combatting cybercrime, serious crimes, or crimes that have big social impact, with national or transboundary spreading, and committed using information systems and modern technical means. Similar to other jurisdictions, the Centre is active in providing assistance and guidance to local police units in cybercrime and electronic evidence matters. The work of the Centre is supported by a cyber lab created within the Technical Criminalist Directorate of the Ministry of Internal Affairs, where technical specialists work on analyses, collection and processing of electronic evidence. The process of forensic examinations takes place in compliance with the provisions of the Criminal Code, the Criminal Procedure Code, methodological materials and other applicable standards.

The National Centre for Personal Data Protection of the Republic of Moldova (NCPDP)

The NCPDP was founded following the adoption of Law no. 17 - XVI of 15.02.2007 regarding the personal data protection. On April 14, 2012, the law was repealed with the entry into force of Law no. 133 of July 8, 2011, on personal data protection. By Law no. 182-XVI of 10.07.2008, the Statute, structure, staff-limit and financial arrangements of the National Centre for Personal Data Protection were approved.

On the basis of these legislative acts, the NCPDP obtained the status of an autonomous public authority, independent from other public authorities, natural persons and legal entities, with the purpose of protecting the fundamental rights and freedoms of natural persons, especially the right for private life regarding the processing and cross-border transfer of personal data[22].

The National Regulatory Agency for Electronic Communications and Information Technology (ANRCETI)

The National Regulatory Agency for Electronic Communications and Information Technology (ANRCETI) is the central public authority that regulates activity in electronic communications, information technology and postal communication, ensures the implementation of development strategies in these sectors, and supervises the compliance of electronic communications and postal service providers with the legislation governing these sectors. The ANRCETI also has the mission to protect the legitimate interests and rights of end-users of electronic communications and postal services by promoting competition in these markets, ensuring efficient use of limited resources, and encouraging efficient investment in infrastructure and innovation. Since April 2016 the Law on Access to Properties and Shared Use of Infrastructure Associated with Public Electronic Communications Networks empowered ANRCETI to ensure the compliance with this law by holders of property rights and electronic communications network and/or service providers when obtaining and exercising the right of access on properties and shared use of infrastructure associated with electronic communications networks.

The National Bank of Moldova

[22] https://datepersonale.md/en/#:~:text=The%20National%20Center%20for%20Personal,into%20force%20of%20Law%20No.

According to Law no. 548-XIII of 21.07.1995[23], the National Bank of Moldova is governed by a Supervisory Board composed of seven members and an Executive Board made up of five members.

In the context of alignment with international standards, the National Bank of Moldova implemented in 2006 a new automated interbank payment system (SAPI). It consists of a real-time gross settlement system for processing urgent and high-value payments and the clearing-based clearing system for processing low-value payments. Thus, a modern payment infrastructure was created, which shaped important premises for the provision of high-quality payment services and the facilitation of non-cash payments. In 2012, Law no. 114 of 18.05.2012 on payment services and electronic money was passed to establish a uniform legal framework for the promotion of efficient and competitive activity on the market for the provision of payment services, issuance and redemption of electronic money, and for the protection of the rights and legitimate interests of payment service users and electronic money holders.

In order to capitalize on opportunities and initiatives to promote new non-cash payment instruments, the National Bank of Moldova established in 2013 the National Payments Council (CNP): a professional high-level consultation forum between various public and private institutions to support the secure and stable operation of the payment system in the Republic of Moldova. The CNP will facilitate the alignment of payment services to market demand and the highest international standards, and help encouraging competition in the cashless payments market so that economic operators and the population benefit from quality payment services at advantageous prices. For the efficiency of funds transfers in the banking sector of the Republic of Moldova during the years 2013-2017, the IBAN code (International Bank Account Number)[24] was implemented for both international and national transfers in order to minimize errors, data processing time and reduce the costs of transfer services.

Office for prevention and fight against money laundering (OPFML) (Financial Intelligence Unit)

The national centre for collection, analysis and dissemination of financial data is also an important synapse between financial sector specialized professional services on the one hand and law enforcement system on the other. This approach makes the mission of the Office for Preventing and Combating Money Laundering extremely important in reducing the vulnerability of banking and non-banking sectors to the risk exposure of money laundering and terrorism financing[25].

As a result of complex analytical processes combined with financial investigations, the OPFML identifies complex schemes and typologies of money laundering and terrorism financing, which are forwarded to operational criminal divisions for examination according to its ability. Taking into account that the success of counteraction of money laundering and terrorism financing requires an efficient and wide level of national and international cooperation, the OPFML cooperates actively and shares information with similar authorities within international organizations such as the EGMONT Group, MONEYVAL, Euro-Asiatic Group, Europol, GUAM. Additionally, the establishment of bilateral relations concerning information exchange with similar counterparts in other countries is a priority, and in this regard 43 cooperation memoranda have been signed.

[23] https://www.bnm.md/en/content/law-national-bank-moldova-no548-xiii-july-21-1995

[24] https://www.bnm.md/en/content/iban

[25] http://spcsb.cna.md /en/page/about

Private sector and academia

The Republic of Moldova, in the development of the national cybersecurity structure, is cooperating with several public and private stakeholders. At the current stage, they are working by establishing agreements and exchanging information in order to ensure the protection of important data for the population and maintain national cybersecurity with market leaders in telecommunication, such as Orange and Moldtelecom, and through effective collaborations with academia in order to prepare high-qualified specialists in cybersecurity: the Technical University of Moldova, the Academy of Economic Studies of Moldova, Police Academy “Stefan cel Mare” of the Republic of Moldova.

“Moldova Cyber Week” a national event dedicated to cybersecurity

Every October, to promote the best cybersecurity ideas and good practices, PI ITSEC annually organizes a national and regional cybersecurity event “Moldova Cyber Week (MCW)” under the patronage of the Government of Republic of Moldova as part of the European Cyber Security Month (ECSM). The MCW is an EU awareness campaign promoting cybersecurity among citizens and organizations on the importance of information security and highlighting steps that can be taken to protect data, whether personal, financial and/or professional. The main goal is to raise awareness, change behaviour and provide resources about how to protect oneself online.

The objectives of the Cyber Security Month are to encourage the public to embrace a more sustained, proactive approach towards online safety and to promote awareness and dialogue about online dangers. Community engagement focuses on dialogue on cybersecurity issues with diverse community members from government entities and industry to academia and non-profits, all of whom would benefit from a collective, hands-on approach to online safety. The mission is to create an open dialog between countries from the region and the international community, which will share their needs and views, to potentially create new measures and law projects, and consolidate the necessary mutual trust between public and private decision-makers and their strategic partners. In the midst of this global strategic puzzle, the event aims to help understand today’s security reality by presenting condensed information in the region and issues in cyberspace. The event presents ideas on how to shield an organization for a secure digital transformation, and aims to produce a multi-stakeholder consortium bringing together the International Community, Government, Industry and Academic interests in an effort to improve the state of cybersecurity on both national and international levels. Regional Cybersecurity outlook has been gained, as well as greater coordination between multiple stakeholders and interaction with European and America-based experts, showcasing innovative cybersecurity practices.

The MCW was first created in 2012, and has since grown into an event gathering over 400 participants and around 50 cybersecurity experts from Estonia, Germany, Latvia, Lithuania, Romania, Georgia, Ukraine, the United States of America (USA), Great Britain, the Netherlands, Switzerland and so on. Recurrent and trusted national and international partners include the USA, the delegation of the European Union to the Republic of Moldova, the International Telecommunication Union (ITU), the Organisation for Security and Co-operation in Europe (OSCE), or the Forum of Incidents Response and Security Teams (FIRST).

Regional forums, webinars, workshops and discussion panels were organized over the last eight years, allowing actors and stakeholders in the country to gather information on topics such as cyber resilience, cyber governance, policy regulation, GDPR, national CSIRTs/CERTs, protection of critical infrastructure, risk management, IoT, digital forensics or cyber-fraud.

For example, in the eighth edition, held on 25-27th November 2020, a series of Online Conference and Webinars on "Building a strong cybersecurity infrastructure in the new normal" was held. On the first day, international experts participated in 13 panels of presentations and discussions addressing important topics for actors in the field. Nearly 3,500 participants watched the event online to learn more about cybersecurity infrastructure in the "new normal" era, key trends for 2020, artificial intelligence solutions, creating efficient ecosystems, regional and international cooperation in the field, as well as the construction of a national cybersecurity capacity stemming from the experiences of other states. On 26-27 November, nine webinars were held on the event agenda, with an average number of 2300 participants. During webinars held by experts from the ITU, EU project "Cybersecurity EAST", Micro Focus, CISO, CLASS-LLC, Thales, GTB Technologies, Kaspersky were discussed with regard to practical solutions in the field of cybersecurity to protect critical infrastructure, response to incidents and threats, cyber executive leadership, investigation of digital forensics, and mitigation of cybersecurity risks in the new normal conditions[26].

Opportunities and challenges in creating a national CERT

Moldova's geographical location and challenges in cybersecurity presents unique opportunities, which would require to have this three-pronged approach:

1. A modern, consolidative approach in the field of cybersecurity is needed, through the elaboration of the Cyber Security Strategy and a set of public policies and normative acts.

2. It is critically important to have updated training of specialists in public institutions in the field of cybersecurity, as well as the need to develop a technical platform for the exchange of information.

3. The most important factor is collaboration: between people, institutions and even states.

Financing such a national CERT structure is very expensive, and at the moment there are no possibilities to allocate financial funds from the state budget to create such a structure. In the 2016-2020 National Cybersecurity Strategy a cost of approx. 49 608 000 MDL (the equivalent of 2.356.820,14 EUR) was established for the development of prevention and urgent response capacities (a national CERT network). In this context and taking into account severe budgetary constraints, the Ministry Finance Committee (MoF) considered it appropriate to create a national CERT on the basis of CERT-GOV-MD, which will exercise its powers at the national level within the approved annual state budget allocations.

This proposal of the MoF, according to ITSEC's argument, is not acceptable, because significant budgetary efforts are needed for the creation of operational capabilities related to a CERT-national entity, which must provide specific functions for the management of information systems security and communications at the national level. Despite many efforts, it has only been possible to cover the high-level central public sector, respec-

[26] www.moldovacyberweek.md

tively within the other state institutions, which are not subordinated to the Government, such as the authorities and institutions within the Local Public Administration, and no cybersecurity activities can be carried out in the private sector. Based on the above and following the approval of Plan of Action for 2019-2024, the creation and designation of an entity that will exercise the role of the cyber incident response centre at national level is a priority objective, involving considerable budgetary allocations. As a precondition for action, deadlines have been established for the elaboration and promotion of the relevant normative framework (2019–2021)[27].

Some of the challenges for creating a national CERT in Moldova are:

- Lack of specialists in the field of cybersecurity qualified in responding to incidents at district and local levels in the country;
- Lack of technical resources for investigating cybersecurity incidents, both in hardware and software;
- Lack of resources in the state budget for the technical service of all public institutions in the country;
- Lack of a national CERT creation strategy: implementation methods from governmental level to national level are not foreseen nor analysed in the current action plan;
- Many processes at local and district levels are still manual or semi-automated, and the staff of these institutions lack an information security management system;
- Lack of initiatives from the current government to motivate specialists in the field of cybersecurity to engage in the public sector;
- Lack of an agreement between the public-private sector regarding the networks and telecommunications on the investigation side and the response to incidents having an impact on national cybersecurity.

Moldova’s cybersecurity collaboration with other countries

The online environment has brought the reality of a borderless society, and the uncertainty of where the next cyber-attack will come from and happen. Some countries have managed to adapt before major national security attacks, while others took action only after they became victims. In order not to fall into the extremes, the process of state automation must go with the same dynamic as cybersecurity measures. There isn’t much cybersecurity in Moldova, but this is only noticeable when the country becomes victim.

Strengthening cybersecurity at the regional level is based on collaboration and exchange of experience and good practices, as only the formation of joint forces can ensure cyber stability. ITSEC has so far signed collaboration agreements on cybersecurity with Georgia, Romania and Ukraine, and at the international level there are memorandums with the cyber incident response teams in Japan and China. Usually, CERT Gov Moldova establishes bilateral agreements directly with national and governmental CERT and CSIRT teams, providing mutual support and information, promoting the same values and objectives such as the integrity, availability and confidentiality of information. In addition,

[27] https://date.gov.md/ro/system/files/resources/2020-03/raport_realizare_pnsc_sem_ii_2019_-_hg_811.pdf

Moldova is a member of the Organization for Democracy and Economic Development (GUAM), along with Azerbaijan, Georgia and Ukraine[28].

The Republic of Moldova is also member of CyberEast[29] - a joint project of the European Union and the Council of Europe, implemented in the Eastern Partnership region by the Council of Europe under the European Neighbourhood Instrument (ENI). Participating countries include Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine. The project aims at adopting legislative and policy frameworks compliant to the Council of Europe Budapest Convention on Cybercrime and related instruments, reinforcing the capacities of judicial and law enforcement authorities and interagency cooperation, as well as increasing efficient international cooperation and trust on criminal justice, cybercrime and electronic evidence, including between service providers and law enforcement. In the region, the Republic of Moldova geographically borders with Romania and Ukraine, and these neighbouring states have a cooperative national cybersecurity strategy.

Moldova also has an Individual Partnership Action Plan (IPAP) with NATO for the period 2017-2019 on political and security subjects such as security and defence sector reform, as well as combating terrorism and ensuring cyber defence. Priority areas for scientific cooperation include cyber defence, environmental security, counterterrorism, energy security, and conducting regional studies related to cross-border activities with the aim of enhancing border security[30]. The Republic of Moldova will continue to implement ongoing SPS flagship activities, including a project to develop a National Action Plan for the Implementation of UN Security Council Resolution 1325 on Women in Peace and Security, a project on "Moldovan Armed Forces Cyber Incident Response Capability (MAFCIRC)," and a project in the area of CBRN defence to mitigate the risk of biological agents.

Closing remarks and conclusions

Given the fact that cyber threats are constantly evolving and becoming more sophisticated and unpredictable, the country must have a flexible and time-sensitive cybersecurity strategy. Due to the cross-border nature of threats, all countries are forced to enter into close international interaction and take into account in their national strategies the possibility of cooperation and exchange of information to combat cybercrime at the regional and international level. Such cooperation is necessary not only for effective preparation against cyber-attacks, but also for timely response to them. Apart from the legislative, normative and technical-normative regulations, a series of specific problems persist related to ensuring the cybersecurity of the Republic of Moldova, and which are component parts of the basic problem identified here:

1. Full security in the processing, storage and access of public data is not ensured, regardless of their classification;
2. Not all networks and services of electronic communications are adjusted to the standards and recommendations of the European Union, the International Telecommunication Union, or to the provisions of the Association Agreement between the Republic of Moldova and the European Union;
3. There are insufficient capacities for prevention and urgent response at national level (CERT);

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

[29] https://www.coe.int/en/web/cybercrime/cybereast

[30] https://mfa.gov.md/sites/default/files/2017-2019_an_ipap_en.pdf

4. The national legislative-normative framework is not fully harmonized with the provisions of the Council of Europe Convention on Cybercrime; the institutions concerned do not have clear competences regarding the assurance of cybersecurity;
5. Lack of education, training and continuous information in the field of cybersecurity;
6. Lack of international cooperation and interaction on identifying risks, vulnerabilities, other events in global cyberspace, and prevention of cross-border cyber threats and attacks.

Recommendations on the implementation of the national informational security strategy would be to allocate necessary human and technical resources for:

7. The training and education of employees within the public sector on cybersecurity;
8. The establishment of a national CERT by training a team of specialists, as well as the provision of hardware and software resources that would allow the investigation of cybersecurity incidents;
9. The support from experts for adapting the framework to the latest regional and international requirements in the field of cybersecurity;
10. Capacity building on incident response for departmental CERTs within public institutions that operate with critical or sensitive data;
11. The creation of a national platform for interaction between the main actors in cybersecurity, to promote best practices and organize workshops and webinars on a regular basis to increase the national capacity in threat hunting, incident response and cyber-fraud investigation.

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