https://doi.org/10.52326/jss.utm.2021.4(1).10
UDC 004.056(478)

CYBERSECURITY OF THE REPUBLIC OF MOLDOVA: A RETROSPECTIVE FOR THE PERIOD 2015-2020

Dinu Turcanu[1*], ORCID: 0000-0001-5540-4246,
Natalia Spinu[2], ORCID: 0000-0003-1659-9962,
Serghei Popovici[3], ORCID: 0000-0002-4302-6003,
Tatiana Turcanu[4] ORCID: 0000-0002-8972-8262

[1, 3 ,4] *Technical University of Moldova, 168, Stefan cel Mare Bd, Chisinau, Republic of Moldova*
[2]*Information Technology Service and Cyber Security, Chisinau, Republic of Moldova*
*Corresponding author: Dinu Turcanu, *dinu.turcanu@adm.utm.md*

Received: 01. 12. 2021
Accepted: 02. 14. 2021

Abstract. The process of implementing information technologies in all areas of economic, political, social life, etc. in the Republic of Moldova has also determined the evolution of cybercrime. New "virtual" dimensions of national infrastructure are being formed, which are becoming more and more important for local and international politics. As a result, in recent years it has been found that computer systems, networks and data are being used more and more frequently for criminal purposes, and the materials that could be evidence of these crimes are also stored and transmitted through these networks by perpetrators. Cybercrime, espionage, propaganda, diversion and excessive exploitation of personal data through electronic communications networks are used as basic tools at all stages of designing a hybrid security threat. Cyberspace-specific threats are characterized by asymmetry and accentuated dynamics and global character, which makes them difficult to identify and counteracted by measures proportional to the impact of the materialization of risks. Moldova is currently facing threats from cyberspace at the address of critical infrastructures, given the increasing interdependence between cyber infrastructures and infrastructures such as those in the financial banking, transport, energy and national defense sectors. The globality of cyberspace is likely to amplify the risks to them by affecting both the sector to the same extent private as well as public. Threats to cyberspace can be classified in several ways, but the most commonly used are those based on motivational factors and the impact on society. In the prevailing conditions cybersecurity is becoming one of the most important areas for ensuring internal security and the effective operation of state institutions in all spheres of social and economic life.

Keywords: *CERT-GOV-MD, computerization, concept, cyber-attack «Digital Moldova 2020», law, National Program, risk management, strategy.*

Rezumat. Procesul de implementare a tehnologiilor informaționale în toate domeniile vieții economice, politice, sociale etc. din Republica Moldova a determinat, de asemenea, evoluția criminalității cibernetice. Se formează noi dimensiuni „virtuale” ale infrastructurii naționale, care devin din ce în ce mai importante pentru politica locală și internațională. Drept urmare, în ultimii ani s-a constatat că sistemele de calcul, rețelele și datele sunt utilizate din ce în ce mai frecvent în scopuri penale, iar materialele care ar putea fi dovezi ale acestor infracțiuni sunt, de asemenea, stocate și transmise prin aceste rețele de către făptași. Criminalitatea informatică, spionajul, propaganda, diversiunea și exploatarea excesivă a datelor cu caracter personal prin intermediul rețelelor de comunicații electronice sunt utilizate ca instrumente de bază în toate etapele de proiectare a unei amenințări hibride de securitate. Amenințările specifice spațiului cibernetic sunt caracterizate prin asimetrie și dinamică accentuată și caracter global, ceea ce le face dificil de identificat și contracarat prin măsuri proporționale cu impactul materializării riscurilor. Moldova se confruntă în prezent cu amenințări din spațiul cibernetic la adresa infrastructurilor critice, având în vedere interdependența crescândă dintre infrastructurile cibernetice și cele din sectoarele bancar, financiar, transport, energie și apărare națională. Globalizarea spațiului cibernetic va amplifica riscurile, afectând atât sectorul public, cât și cel privat. Amenințările la adresa spațiului cibernetic pot fi clasificate în mai multe moduri, dar cel mai frecvent sunt clasificate pe baza factorilor motivaționali și impactul asupra societății. Astfel, în condițiile actuale securitatea cibernetică devine unul dintre cele mai importante domenii pentru funcționarea eficientă a instituțiilor de stat în toate sferele vieții sociale și economice.

Cuvinte cheie: *CERT-GOV-MD, computerizare, concept, atac cibernetic «Digital Moldova 2020», lege, Program național, managementul riscurilor, strategie.*

Introduction

In international practice cybersecurity is defined as a set of tools and principles for ensuring and guaranteeing security, which is a single concept of risk management, mean the application of the necessary technologies and actions to protect the information system and the user's environment. When the state acts as this user, the problem of cybersecurity becomes one of the key elements of ensuring national security. At the same time, it is obvious that cybersecurity should be considered as one of the main components of national and international security in general, and crime in this area is often closely related to other types of threats, including industrial espionage, activities of foreign intelligence services, international terrorism, etc.

Another feature of cyber threats nowadays is the rapid development of information technologies, which provides more and more tools for committing crimes, they are becoming more sophisticated, more technological, and in this regard, the damage they can cause increases many times over. This also requires government agencies involved in countering cybercrime to be prepared for new challenges and constantly improve methods and ways to combat cyber threats. An additional difficulty for them is created by the fact that cyberspace has no borders, and interested players (special services of various states, criminals, terrorists, cyber fraudsters, hackers, industrial spies, etc.) can create threats from anywhere in the world and of a very different nature. This creates difficulties in identifying the source and nature of threats in cyberspace.

In fact, today in the world there is already a real war in cyberspace for political, economic and criminal purposes. Even more dangerous, this war is being fought without a clearly defined "battlefield" and without rules. In this context, the Republic of Moldova, as a state, should build its cyber security strategy taking into account all these factors and features.

1. Information security concept of the Republic of Moldova

The small size of the territory and the rather developed internet infrastructure of the Republic of Moldova facilitate the activities of special state bodies to counter cyberattacks. But this also creates additional problems associated with the growing level of internet penetration and the assimilation of information technologies by an increasing number of users. In these conditions, ensuring cybersecurity becomes one of the key tasks of the state.

For the first time at the legislative level, the issues of information security and conditions of activity in the information space were established by Law No. 467 of November 21, 2003 "On Informatization and State Information Resources [1] with subsequent amendments and additions. In this document, the interpretation of the basic terms used in the field of information security appeared. However, Moldova really began to deal with cybersecurity issues after 2009, when protests and riots after the April 2009 elections were called by many a “Twitter-revolution”. In 2010, a state body, the Center for Cybersecurity (CERT-GOV-MD), was created, which became part of the State Enterprise Center for Special Telecommunications - a structural unit of the Information and Security Service of the Republic of Moldova.

The creation of CERT-GOV-MD entailed a number of other actions to ensure comprehensive protection of state interests from cyber threats. In the same year 2010, the General Prosecutor's Office of Moldova created a specialized Cybercrime Investigation Unit, and the Information and Security Service created a Cybercrime Unit. Then in 2012, the Ministry of Internal Affairs also created its own Cybercrime Unit. Thus, was created an institutional hierarchy to ensure cyber security in Moldova and counteract attacks on the information resources of the state. However, the legislative base required further improvement. And in the period 2015-2020, serious steps were taken in this direction, which created the current regulatory framework for the integrated support of cybersecurity in the Republic of Moldova.

This regulatory framework was set by the Government Decision No. 857 of October 31, 2013, which approved the National Strategy for the Development of the Information Society “Digital Moldova 2020” [2], as well as the Action Plan for its implementation. The strategy describes in detail the current situation in the field of information security at that time and refers to the legal framework governing this area. In paragraph 10 of Art. 2.1 of the document is underlined; “In the international ranking of the level of ICT development (IDI index), the Republic of Moldova ranks 62nd among 155 countries (4th among the CIS countries), and in terms of the level of e-government development (e-GRI index), it ranks 69th among 159 countries, moving up 11 positions compared to 2010, but at the same time taking the last place among the countries of Eastern Europe” [2].

In the same document in paragraph 36 of Art. 3.4 “The threat of growing cybercrime and the risk of decreasing confidence in networks and online services” states the following: “Currently, there is no state body in the Republic of Moldova directly responsible and empowered with powers, functions and responsibilities in the field of cyber security. At the moment, there are a number of institutions involved in this process, each of which is responsible for relevant issues in its segment of activity. In this regard, it is necessary to fill the existing gap in the regulatory framework in the field of cyber security.

In chapter 4.3 of the Strategy, entitled “Safe and Secure Digital Environment”, among the specific tasks under the first item is: “increasing the level of cybersecurity of critical national infrastructures (government agencies / institutions, electronic communications networks, water pipelines, energy systems, transport networks, etc.).

The document provides a wide range of government actions to increase the level of cybersecurity of national infrastructures. Including the addition and harmonization of the regulatory framework, the interchange of information at the public and private level about information threats and risks, the introduction of electronic identity management to ensure cybersecurity, etc. Among other things, it is also envisaged to “strengthen the CERT-GOV-MD team (creation CERT-GOV-MD structures / commands at national level) [2].

The adoption of the National Strategy "Digital Moldova 2020" and the Action Plan for its implementation became the starting point that significantly intensified the activities of state bodies to improve the cybersecurity of the Republic of Moldova and the introduction of information technologies in all spheres of public administration. Moreover, in the Action Plan, all activities, funding sources, responsible authorities and implementation dates were phased out, which stimulated activities to implement the goals and objectives of the National Strategy.

Of course, the implementation of this document in full demanded a significant update of the regulatory framework in the field of cybersecurity, especially since the rapid development of information technologies and growing threats in cyberspace required an adequate response from government institutions.

The most significant documents on ensuring information security in Moldova include, first of all, the Concept of Information Security of the Republic of Moldova [3], approved by Law No. 299 of December 21, 2017 and which came into force after being officially published in February 2018. In art.8 of part 1 of the document clearly sets out the national interests of the Republic of Moldova in the field of information security: "8. National interests in the field of information security are: ensuring the observance of rights and freedoms regarding access to information resources; development of the spheres of information technology and electronic communications and the expansion of their use; ensuring the protection of the information space, vital and strategically important facilities, critical infrastructure, information classified as state secrets, and information of limited access; prevention, detection and suppression of risks and threats to the information security of the Republic of Moldova, as well as protection of the national information space and society as a whole from the impact of external and internal propaganda and media aggression ".

In the same document, in part 2, among the basic concepts used in relation to the Concept of Information Security, the following is emphasized: "the policy of ensuring information security of the Republic of Moldova is a set of activities of public administration bodies, their duties and responsibilities for protecting national interests in the information space, based on maintaining the balance of interests of the individual, society and the state" [3].

2. Strategic goals and objectives of ensuring cybersecurity in the Republic of Moldova

No matter how timely and voluminous the documents adopted by the Parliament and the Government of the Republic of Moldova in the field of cybersecurity are, the rapid development of information technologies and the growth of related cyber threats force us to constantly improve the regulatory framework in this area.

Moreover, the signing in 2014 of the Association Agreement between the Republic of Moldova and the European Union set new tasks for the country to harmonize its domestic legislation with European directives in this area. In this context, a significant role was played by the Government Decision No. 811 of 29.11.2015 "On the National Cybersecurity Program of the Republic of Moldova for 2016-2020" [4]. The document clarifies the key terms and concepts in the field of cybersecurity and their meanings, as well as defines the basic principles on which the concept of ensuring the country's cybersecurity is based.

Also, for the first time in the document, the term "management" appears in relation to cybersecurity systems. In particular, the first article of the Program emphasizes: "The goal of the National Cybersecurity Program of the Republic of Moldova for 2016-2020 (hereinafter - the Program) is to create a cybersecurity management system in the Republic of Moldova by ensuring the security of information society services, thus contributing to the development of an economy based on knowledge, which in turn will stimulate the growth of the level of economic competitiveness, social unity, as well as ensure the creation of new jobs".

Assessing the current situation with cybersecurity and countering threats in the information space at that time, the Program points to the existing problems with identifying and accounting for such threats. In particular, clause 7 of Section II of the document reads: "7. So far, not a single cybersecurity audit has been performed, there are no studies or reports detailing the situation regarding information crime in the Republic of Moldova, cyber threats and risks, cyber-attacks and incidents, other events that have occurred in cyberspace, the number of victims and economic losses due to their materialization”[4], [5].

Further, the document analyzes in detail the reasons why the cybersecurity system in Moldova does not yet meet the challenges of the time. In particular, the Program notes that the main problems in this area include the lack of a cybersecurity management system, as well as the identification of vulnerabilities and risks due to audit. As a result, Moldova does not have a complete picture of the crimes committed in cyberspace, which makes it difficult to develop effective countermeasures. But one of the main problems in ensuring cybersecurity is indicated in paragraph 15 of the same section: “15. Until now, there is no legal framework regarding the delineation and coordination of the competences and responsibilities of public and private institutions in the field of cybersecurity, a mandatory cybersecurity audit mechanism is not applied, through which cyber vulnerabilities, risks and threats can be identified in order to prevent or mitigate using special measures attacks, incidents and other events that have occurred in cyberspace, the origin of which is difficult to determine”.

The measures to be taken to improve the situation and bring the regulatory framework of Moldova in line with the European directives in this area are set out in section IV “Actions to be taken to achieve the goals”. It notes that all actions and measures should be systematized and reflected in the Action Plan for the implementation of the National Cybersecurity Program of the Republic of Moldova. For each of the specific tasks contained in the Program, various implementation mechanisms are provided.

Among them, paragraph 24 says: “24. The specific task “Development of capacity for prevention and emergency response at the national level (national CERT network)” will be achieved by creating a National Cyber Security Incident Response Centre (CERT) and departmental centers in central public authorities management, local public administration authorities, other structures that have state information systems, establishing obligations for mandatory operational reporting and accounting of cyber security incidents for central and local public administration authorities and the business environment in the field of information technology and communications, developing and applying methods for early prevention of incidents cyber security of the Republic of Moldova, conducting practical exercises and trainings to strengthen the ability to respond to cyber incidents and attacks with their blocking, including through other activities in accordance with the Action Plan ” [4].

This position has been developed in other conceptual documents in the field of cybersecurity. The Parliament of the Republic of Moldova, by its Resolution No. 257 of 22.11.2017, approved the new "Information Security Strategy of the Republic of Moldova for 2019-2024" and the Action Plan for its implementation [6]. This document also focuses on the need to create an integrated system for reporting and assessing information security threats and developing rapid response measures. The following are named as priority actions for the implementation of this provision:

1) Establishment of the National Cybersecurity Incident Response Centre (national CERT);
2) Designation of a body to act as the Governmental Cyber Security Incident Response Centre (CERT Gov);
3) Strengthening collaboration between National CERT, Governmental CERT and private CERTs [6].

In order to implement these priorities and develop the institutional system for ensuring cybersecurity, the Government of the Republic of Moldova adopted Resolution No. 414 of 08.05.2018 “On measures to consolidate data centers in the public sector and rationalize the administration of state information systems” [7]. The key decision of this decree was the reorganization of the state enterprise "Center for Special Telecommunications" into the Public

Institution "Information Technology and Cyber Security Service". The state enterprise "Center for Agricultural Information" also became part of this institution by way of takeover. By this resolution, the Government also approved the Charter of the Service and its areas of competence. In particular, the following are named among the functions of the Public Institution:

1) creation, management, maintenance and development of information technology infrastructure and telecommunications system of public authorities as part of a special communication network;
2) creation and management of centralized telecommunication infrastructure and data transmission centers and their development;
3) implementation of technical and technological duties of state electronic services;
4) implementation and provision of cybersecurity of information technology infrastructure and telecommunications system of public authorities in accordance with the mandatory minimum cybersecurity requirements established by the Government and the best international practices in this area;
5) implementation of policy documents in accordance with the established objectives and regulations in the field of cybersecurity [7].

The implementation of the provisions of this Government Decree allowed in a short time to radically rebuild the entire cybersecurity infrastructure of the country and build a clear hierarchical line of responsibility of various state bodies for the creation and development of information resources. In addition, the document made it possible to centralize the management of the telecommunications infrastructure and create a single technological platform for the provision of electronic services by public services. However, two years later, the Cabinet of Ministers of Moldova was forced to adopt amendments and additions to this Decree in order to further specify the functions and responsibilities of the Information Technology and Cyber Security Service, as well as expand the list of measures to ensure the cyber security of the Republic of Moldova. By Government Decree No. 482 of 08.07.2020. the "Measures necessary to ensure cyber security at the government level" were approved, as well as amendments were made to Resolution No. 414/2018, which was mentioned above. By this document, the Public Institution "Information Technology and Cyber Security Service" is designated as the Governmental Centre for Response on Cybersecurity Incidents [8], [9]. In addition, in order to fulfil the measures specified in the Resolution, the following definitions are introduced:

CERT Gov - Governmental Centre for Response on Cybersecurity Incidents, an entity that serves as a single point of communication and reporting of cyber security incidents of the Government and has the capacity necessary to prevent, analyse, detect and respond to cyber incidents at the government level;

Departmental CERT - a subdivision or responsible person appointed within public entities that own the infrastructure / systems of information technology and communications and that have the capacity necessary to maintain mandatory operational records and reporting of cyber security incidents.

CERT Gov is responsible for: ensuring the implementation of incident prevention and response policies in cyber infrastructures according to its competence; providing an organizational basis and technical support for the exchange of information between various groups such as CERT, users, public entities; interaction with structures of the CERT type within the framework of public entities with regard to the procedure for reporting, storing and processing information related to incidents and threats to information security; identification, registration, classification and analysis of cyber security incidents, etc.

At the same time, clause 13 of Section IV of the Government Decree specifically stipulates that, as part of the implementation of the measures provided for by the document, CERT Gov and public entities process personal data in accordance with the legislation on the protection of personal data.

3. Cybersecurity threats and needs in Moldova in 2020

As a society that runs more largely on technology, we also as a result depend on it. The Republic of Moldova is in a continuous process of strengthening cyber security at the national level, both from a legal, institutional and procedural point of view, and efforts are being made in this regard by the authorities with responsibilities in the field.

In the general context of cyber security discussions, at 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. Since the establishment of a governmental CERT structure took place only in 2020, the annual record of cyber incidents so far has been executed by the department of cyber incident response center within ITSec, only for national analysis and study.

From the data collected in the past 5 years, we could identify the vectors of attack changing through the years in the same trend with the nearby regions, a fact confirmed by the reports published by ENISA regarding the threats landscape. For example, in Moldova there was identified a tendency of malware infestation of business and corporate e-mails which aim at compromising security systems by exploiting the human factor. According to a study from 2019 [10] by ENISA, 94% of all malware types were delivered via e-mail [11]. The top five strains of malware targeting businesses were: Trojan.Emotet, Adware, InstallCore, HackTool. WinActivator, Riskware. BitCoinMiner and Virus, Renamer (Figure 1). Ransomware attacks targeting the public sector increased in 2019 because of its ability to pay higher ransoms.

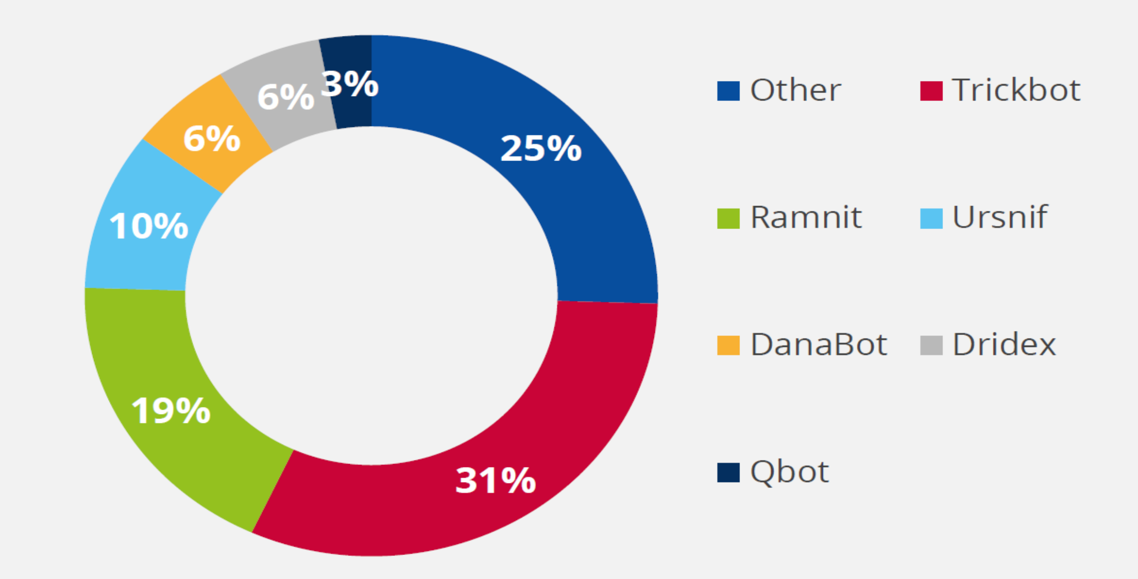

Figure 1. Global malware detections in 2019 CheckPoint [12].

From the data collected by CERT-GOV-MD in cooperation with Shadowserver Foundation and CERT-Bund [13], [14] processed at least 43334 reports on malware activity in the country, including 27879 reports being government networks which represent 64,33% from the total of malware activity, this rate indicates that the attack vectors targeted the government infrastructures.

Lately in 2018, for example the trend of cyber-attacks in Moldova, could be classified in 5 most common incident classes in order of frequency of alerts: vulnerable system, compromise system, botnet, malware, attack. In Figure 2 represented below is a data chart, indicating the number of malware files identified as attachments to corporate emails that were blocked between 2015-2019.

Ransomware attacks have been dethroned by unauthorized cryptocurrency mining activities, mainly by exploiting vulnerabilities in websites or network equipment (cryptojacking). However, the risks associated with cyber-attacks on IT & C infrastructures with critical values for national security remain largely exacerbated by the existence of technical, procedural and human vulnerabilities [15].

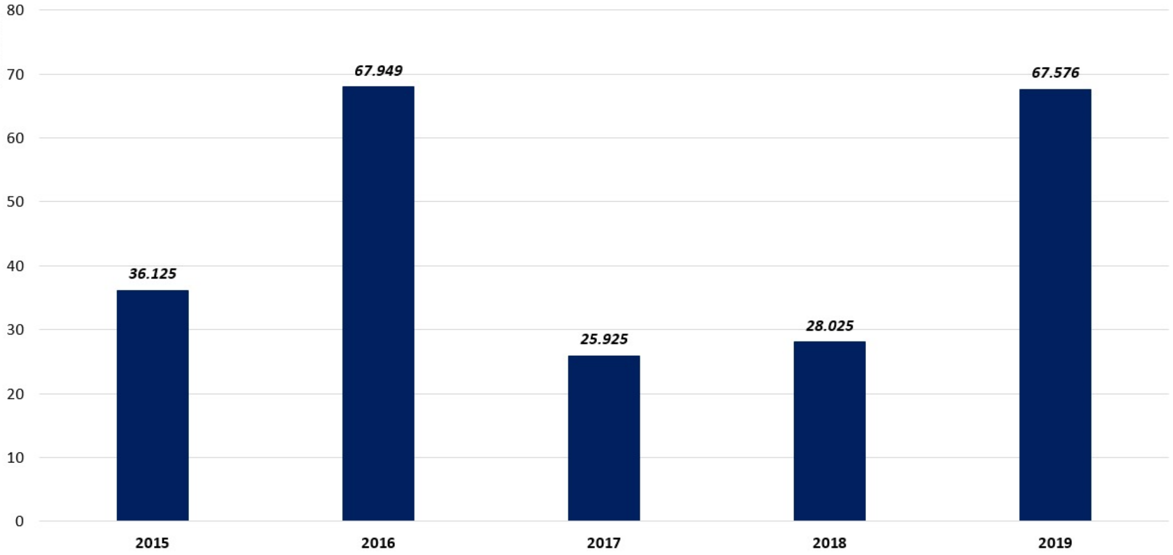

Figure 2. Malware detections in emails attachments between 2015-2019.

For example, during 2018 (Figure 3) in cyberspace allocated to public authorities and private companies of the Republic of Moldova were registered 127 418 information systems and telecommunications networks infected with various types of malware that form a malicious botnet information infrastructure (level 4 and 3).

Most infected information systems are located in Chisinau (58.92%), Tiraspol (30.72%), Bendery (3.38%), Balti (1.36%). These were directed by approx. 764 control and routing (C&C) servers located in 44 countries around the world. Most routing servers were located in: United States (30%), Germany (19%), Sweden (14%).

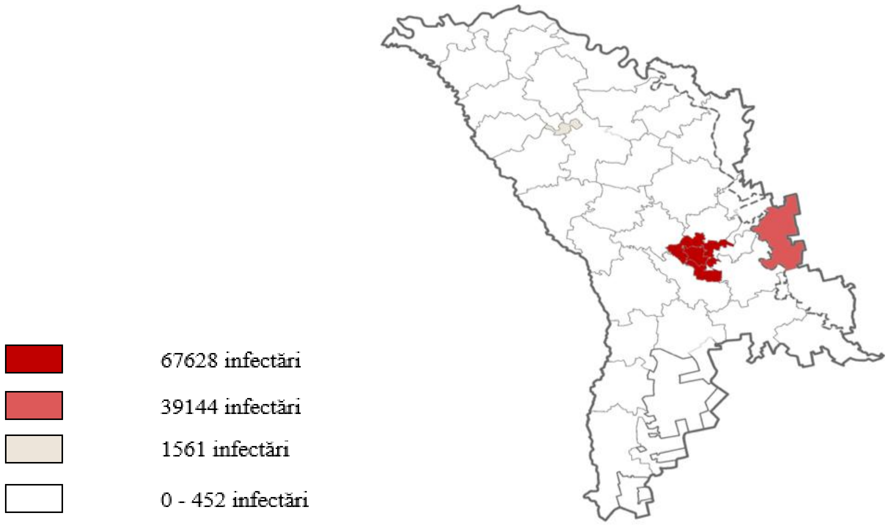

Figure 3. Location of information systems and telecommunication networks infected by regions on the territory of the Republic of Moldova in 2018.

The main objective of the offensive actions carried out by these actors, remains the exfiltration of information of strategic interest, the type of attack through which it realizes this being Advanced Persistent Threat (APT). Elements of modus operandi such as social engineering, spear-phishing, multiple levels of command and control servers or vulnerability scanning, continue to be some of the most used techniques to meet the objectives of these actors [16].
Analyzing the infected information systems and telecommunications networks were identified cca.108 different families of malware. The most dominant were: wannacrypt (31%), pykspa (22%), mkero (7%), andromeda (6%), monerominer (5%), sality + sality-p2p (5%), android. fobus - 3540 (3%) infections (Figure 4).

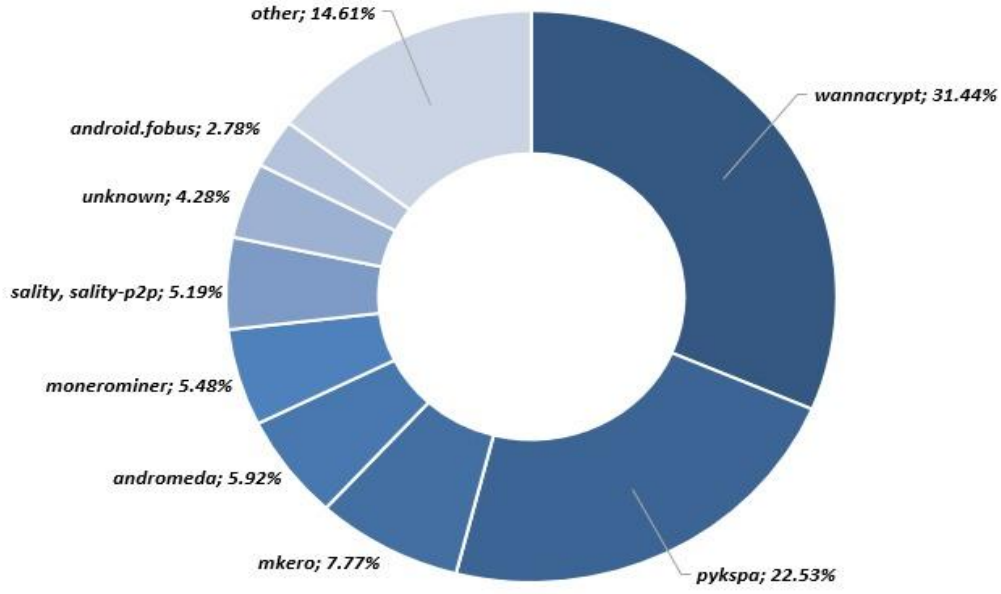

Figure 4. Family of registered malware.

Many of the cyber defense systems used by critical infrastructure operators in the Republic of Moldova are outdated and inefficient to prevent possible attacks. In the absence of adequate measures and coordination of critical infrastructure security efforts, these systems remain extremely vulnerable, with unauthorized persons gaining control over systems vital to the functioning of a state. In this sense, it is absolutely necessary that the field of critical infrastructures be periodically analyzed, monitored, evaluated and optimized, starting a process of identification of critical infrastructures at the level of public administration.

In order to ensure a strong cybersecurity in Moldova, we need to invest resources in many segments as following:

- Harmonizing the legislative framework with european and international requirements and tendencies on cybersecurity;
- Professional training in the field and the realization of some actions of awareness / understanding of the field at the level of the decisional factors within the 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 ensure mobile groups for incident response;

- Opening up communication channels, setting up working groups and public consultation, involving civil society and public-private partnerships are becoming key directions on which public policies must focus.

Conclusions and recommendations

Cyberspace became increasingly important both for the functioning of states and for the provision of public services to citizens. It is crucial to realize that cyberattacks cause economic damage, undermine public confidence in online services, and cause real harm to government, business, citizens, their property and privacy.

Proceeding from this, any state is obliged, in order to ensure cyber security, to take comprehensive and consistent measures to develop the state cybersecurity system. This also involves conducting an audit and creating a mechanism for updating requirements and recommendations for cybersecurity in relation to state and municipal information systems, telecommunications networks, and other infrastructure. It is necessary to constantly and systematically improve the legislation of the Republic of Moldova in the field of cybersecurity, including on the basis of adapting the legal norms of European states, bringing the regulatory framework in full compliance with the international agreements ratified by Moldova.

Given the fact that cyber threats are constantly evolving, becoming more sophisticated and unpredictable, the country must have a flexible and time-sensitive cybersecurity strategy. In addition, 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 in order to combat cybercrime at the regional and international level. Such cooperation is necessary not only for effective preparation for cyber-attacks, but also for timely response to them.

References

1. (2004) LEGE Nr. 467 din 21-11-2003 cu privire la informatizare şi la resursele informaţionale de stat
2. (2013) HG Nr. 857 din 31-10-2013 cu privire la Strategia naţională de dezvoltare a societăţii informaţionale “Moldova Digitală 2020
3. (2018) LEGE Nr. 299 din 21-12-2017 privind aprobarea Concepţiei securităţii informaţionale a Republicii Moldova
4. (2015) HG Nr. 811 din 29-11-2015 cu privire la Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020
5. National Association of Regulatory Utility Commissioners (2018) Cybersecurity Strategy Development Guide
6. (2019) Hotărâre Nr. 257 din 22-11-2018 privind aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019–2024 și a Planului de acțiuni pentru implementarea acesteia
7. (2018) HG Nr. 414 din 08-05-2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat
8. Brett M (2019) Cyber Incident Framework Article Oct19 V01.pdf. 87932 Bytes. https://doi.org/10.6084/M9.FIGSHARE.9963767
9. Kalakuntla R, Vanamala AB, Kolipyaka RR (2019) Cyber Security. HOLISTICA – Journal of Business and Public Administration 10:115–128. https://doi.org/10.2478/hjbpa-2019-0020
10. The European Union Agency for Cybersecurity (ENISA) (2020) ENISA Threat Landscape 2020 - Malware
11. Mutemwa M, Mouton F (2018) Cyber security threats and mitigation techniques for multifunctional devices. In: 2018 Conference on Information Communications Technology and Society (ICTAS). IEEE, Durban, pp 1–6
12. Check Point Research (CPR) (2020) CYBER SECURITY REPORT. Check Point Research (CPR)
13. Federal Office for Information Security (2014) CERT-Bund Reports
14. Turcanu, Dinu, Popovici, Serghei, Turcanu, Tatiana (2020) DIGITAL SIGNATURE: ADVANTAGES, CHALLENGES AND STRATEGIES. https://doi.org/10.5281/ZENODO.4296327
15. Hajri HHA, Mughairi BMA, Hossain MI, Karim AM (2019) Crypto Jacking a Technique to Leverage Technology to Mine Crypto Currency. IJARBSS 9: Pages 1220-1231. https://doi.org/10.6007/IJARBSS/v9-i3/5791
16. Alqatawna J, Hadi A, Al-Zwairi M, Khader M (2016) A Preliminary Analysis of Drive-by Email Attacks in Educational Institutes. In: 2016 Cybersecurity and Cyberforensics Conference (CCC). IEEE, Amman, Jordan, pp 65–69