Information & Security: An International Journal

Natalia Spinu, vol.32, 2015 http://dx.doi.org/10.11610/isij.3208

CREATING AND STRENGTHENING CYBERSECURITY IN THE REPUBLIC OF MOLDOVA

Natalia SPINU

Abstract: Like most of the countries, Republic of Moldova faced the need of protecting its cyberspace against emerging cybersecurity threats. The lack of coordination between responsible institutions, established cybersecurity mechanisms, and well-trained specialists made private companies and public institutions an easy target for cyber attacks performed by malicious actors like hacktivist groups, terrorist organisations and state-sponsored companies. The consequences of such attacks damage reputation, business processes and affect the image of the country on the international scene. This article shares the experience of Moldova in the efforts of planning and building cybersecurity. It is written from the point of view of Moldova's Cybersecurity Centre – CERT-GOV-MD, whose governmental status and active involvement in national cybersecurity development processes allow to provide a broad overview of different situations, in which Moldova and its state institutions found themselves, and the problems faced along the road to achieving the stated goal. In this regard, the article covers the period from the initiation of building cybersecurity until the most current results.

Keywords: cybersecurity, cyberspace, legal base, law enforcement, institutions, Republic of Moldova.

Introduction

The revolution in information technologies created a new form of human organisation—information society—where the majority of people are engaged in activities related to creation, distribution and use of information. As these activities are carried out in a non-physical world, or "cyberspace," regular state governance measures for its protection are not suitable, which creates significant risks to national security. That is why protecting cybersecurity is a primary task of a state for ensuring safety and prosperity of a country. The purpose of the current work is to share experience from building cybersecurity in the Republic of Moldova. To achieve this purpose, the article describes the evolution of cybersecurity measures undertaken after Republic of Moldova gained independence.

Definitions

As the article is intended to reach a wider audience of readers from various fields, related to information technologies, the author considers an explanation of the notions used in this text a precondition in order to establish common understanding.

What does "to create cybersecurity" mean at the level of the state? The "cyber" prefix is associated with the national cyberspace, composed of interconnected and interrelated digital information, information systems and telecommunication infrastructure that are in possession of a particular nation. Further, "security" is understood as a protection mechanism. Protection mechanisms can vary from a lock on the door to a server room to a special telecommunication traffic-filtering device, but at the state level, it represents a set of legislative, persuasion and enforcement measures at disposal of the government in the area to be protected. In this regard, the author defines "cybersecurity" as a state-level protection mechanism applied to the national cyberspace in order to prevent its abuse. Accordingly, "to create cybersecurity," at the level of the state, means to establish a mechanism for protecting the interconnected and interrelated digital information, information systems and telecommunication infrastructure, possessed by a nation, by planning and implementing specific legislative, persuasion and enforcement measures.

Legislative measure is defined as a legal act, which can take the form of a law or a by-law. Examples of legislative measures include, e.g. cybercrime law, various regulations, information security standards, cybersecurity strategies and plans. For its part, persuasion measure is regarded as a method of direct or indirect influence on the consciousness of the society or part of it, such as education, training, awareness, capacity and cooperation building. In the context of the current article, enforcement measure is defined as an act of a specialised authority, the duties of which include monitoring and enforcing compliance with approved legislative measures.

Finally, a cybersecurity incident is an act of abuse of the cyberspace. This term should be distinguished from the term "cybercrime." In this regard, a cybersecurity incident is regarded as "a minor crime" – a crime, which does not have serious impact on digital information, information systems or telecommunication infrastructure, and does not create risks for human life.

Developments in 1991 – 1996

After USSR's dissolution in 1991 then newly formed Moldavian state faced the immense challenge of transition from a centrally-managed to a free market economy. Among other things, the transition required the creation of a common information space, based on modern technologies, developed information society and definition of principles for the involvement of the state in these processes. The situation was complicated by the fact that the development of the information society in Moldova was lagging 6 to 18 years, depending on the economic sector, behind the developed countries, which was coupled with the lack of legislation in the area of information technologies. This hindered development and made the national economy less competitive.

At the same time, in spite of 6853 existing computers in the country as of 1 January 1993, it was not possible to form national cyberspace due to the lack of a general-purpose data network. A similar situation was found at the level of public administration where the majority of information systems worked autonomously, as most of them were incompatible with each other from information exchange point of view.[1]

In order to change the situation, the government of Moldova elaborated and approved decision No. 415 of 5 July 1993 on the establishment of a multi-year development programme, involving a concept for society informatisation and mechanisms for its implementation, which proclaimed basic principles, priority areas and key stages of its realisation.[2] The concept envisaged, among others, the adoption of legislation to regulate the process of informatisation, the creation of a national data transmission network, and the modernisation of computer equipment production. It was expected that the first results would be achieved within 1-2 years of the document's adoption.

It took the government one year and eight months to finally approve in 1995 the draft of a concept for society informatisation. By then the situation in the national economy deteriorated which, together with uncontrolled privatization, led to irreversible consequences for the hi-tech industry. Soviet-era defence plants with potential to produce micro- and optical electronics, which were supposed to be a main driving force of the informatisation process in the country, were restructured to produce metal products like doors, gates and fences. As a result, unique technological equipment and capacities were lost.[3] That demonstrated lack of governmental capability to lead the society informatisation process. From that moment on, the process developed spontaneously and was mostly driven by business interests.

The Years 1997 - 2002

As of 1997, 170 companies formed the country's information sector. They utilised about 14 000 computers connected in more than 200 local and regional private networks, and in four public networks. Around 17 providers connected to the Internet nearly 1 800 subscribers located in the capital, while the rest of country's was not able to connect with world's cyberspace.[4] At the same time, the information systems of the state institutions remained autonomous, without being connected among each other or with the Internet. This hindered operative information transfer and as a result impeded the improvement of the efficiency of public administration authorities.

The solution to that problem was found in 2000, when a proposal, developed by the non-governmental organisation “MoldInfoNet,” in close cooperation with the Ministry of Economy, won a tender for the implementation of a Republican Computer network for data transfer, organised by the United Nations Development Programme as a part of the “MOL/97/011 Strengthening Local Governments II” project. The implementation of the project allowed to interconnect, during 2001-2002, state institutions across the country into a single informational computer network, named “Governmental Intranet,” and to equip information centres of the State Chancellery, ministries, departments and district centres with modern equipment and software.[5]

The establishment of a “Governmental Intranet” brought to the state institutions not only benefits in the form of access to the Internet, e-mail and specialised information databases, but also posed cybersecurity risks to important state information transmitted and processed within the network. To ensure secure exchange of information within the “Governmental Intranet,” the government of Moldova adopted decision No. 735 of 11 June 2002 “on special telecommunication systems of the Republic of Moldova,” which led to the establishment of State Enterprise “Centre of Special Telecommunications” (S.E. CTS), subordinated to the Intelligence and Security Service.[6] From that moment, S.E. CTS started playing a key role in providing telecommunication services for and ensuring cybersecurity of state institutions.

Cybersecurity Developments from 2003 to 2012

Year 2003 was marked by a rapid growth of the telecommunications and information sector. That was largely a result of significant investments of private companies in the development and modernisation of the telecommunications infrastructure. The number of Internet users increased from 0.03 per 100 citizens in 1997 to 8 per 100 citizens in 2003. At the same time, many issues remained unresolved and new ones emerged. ICT-related legislation was largely missing, while existing laws and regulations had many flaws and were not able to fulfil their mission. At the same time, highly qualified specialists were leaving the country due to the low salaries.[7]

By 2004, it became clear that further social-economic development of the Republic of Moldova and solving existing problems was impossible without building an information society. Therefore, the President of Moldova, by his Decree No. 1743 of 19 March 2004 ordered to recognise its creation as a national priority and to develop a national strategy for the development of information society and an action plan for its realisation.[8] The latter documents were subsequently adopted on 9 March 2005. As the information society highly depends on underlying information technologies, the action plan envisaged the elaboration of legislative and enforcement measures, which later formed the groundwork for ensuring cybersecurity in the Republic of Moldova. In 2007, the law “on electronic communications” was adopted. It obliged providers of electronic communications to store for six months, for Internet traffic, all available information received or processed during service provision, which could permit to identify source, destination and circumstances of communication.[9] That allowed competent authorities to request collected data for cybercrime investigations.

Another achievement of 2007 was the realisation of the Moldova-NATO project "Creation of Infrastructure for CERTs in Belarus, Moldova, Ukraine and their Initial Operation," which allowed the establishment within the non-governmental National Research and Educational Network of Moldova (RENAM) of a prototype computer security incident response team – MD-CERT. The team took responsibility for handling information security incidents and offering other cybersecurity services to state educational and science institutions, connected to RENAM's telecommunication network.[10]

Later, the Parliament of Moldova ratified Budapest convention on cybercrime by means of adopting Law No. 6 of 2 February 2009. Territorial application of the convention allowed the creation of a common, for all signatories, criminal policy aimed at the protection of society against cybercrime, by adopting appropriate legislation and fostering international co-operation.

Some requirements of the Budapest Convention were fulfilled through the adoption of a second legislative measure (also envisaged by the action plan) – Law No. 20 of 3 February 2009 "on preventing and combating cybercrime." The law defined the competent bodies in the area of combating cybercrime, notions, responsibilities of service providers and principles of international cooperation. According to the law, the responsibilities for preventing and combating cybercrime were assigned in the following way:[11]

- Ministry of Interior: conducts investigations, realises criminal prosecution, identifies persons who committed a cybercrime, maintains records of investigated cases and carries out international cooperation;
- Intelligence and Security Service: conducts investigations of cybercrimes, which threaten national security, identifies international criminal organisations and maintains records of investigated cases;
- General Prosecutor's Office:
    a) coordinates, conducts and performs criminal prosecution, as provided by law;
    b) orders—on request of criminal prosecuting authority or on its own initiative—the immediate preservation of computer data that is in danger of being destroyed or altered;

c) represents the prosecution on behalf of the state in courts as prescribed by law.

- Ministry of Information Technologies and Communications together with Intelligence and Security Service: develops proposals on securing computer data;
- National Institute of Justice: performs professional education of persons engaged in execution of justice in the area of cybercrime.

In the same year, amendments to Code No. 985 of 18 April 2002 “Criminal Code of the Republic of Moldova” came into force, which defined notions, types of cybercrimes and possible punishments.[12]

However, adopted legislative measures had many flaws that led to problems in their implementation. For instance, the law on electronic communications contained a too broad requirement “to store all available information,” which created a problem for the service providers, obliged to keep as large volumes of data as possible thereafter. For its part, the law on preventing and combating cybercrime regulated in a far too general manner the responsibilities of the institutions involved in the investigation, which led to uncertainty as to which institution was in charge of carrying out an investigation. At the same time, effective cooperation of competent authorities was hindered by the fact that the law only listed participants and types of cooperation without putting down specific responsibilities, criteria and means of information exchange, what made inter-institutional cooperation more voluntary in nature.

The inability of the existing criminal justice system to deal with the new types of crimes created another problem. As compared to a regular crime, cybercrime differs in a variety of ways:

- Cybercrime happens in a non-physical world, so there are no living witnesses; it is harder to collect evidence and trace an attack; special equipment is required for an investigation;
- The offender and the victim can be geographically separated. A cybercrime can happen at the territory of one country, while the offender could be located on the territory of another country. This creates problems related to jurisdiction, evidence collection and criminal prosecution, making overall success of the investigation very much dependent on the effectiveness of international cooperation.
- As dealing with cybercrime demands extensive knowledge and understanding of the technical aspects of the nature of cyberspace, specially trained staff is required for successful execution of criminal justice process phases (investigation, prosecution and adjudication).

These specifics necessitated significant changes in the structure of the criminal justice authorities, establishment of international cooperation mechanisms, and provision of specialised education and training for those in charge for dealing with cybercrime.

In order to address those needs, specialised units—*Division for Cybercrime Investigation* and Research and *Department for Combating Cybercrime*—were established in 2010 within the General Prosecutor's Office and the Intelligence and Security Service, respectively. That allowed to delegate the responsibilities for implementing the law on preventing and combating cybercrime to the newly formed units and to meet the requirement of the Budapest Convention on Cybercrime by establishing a 24/7 national contact point.

In the same year, by implementing Government Decision No. 746 of 2010 "On the approval of the updated Individual Partnership Action Plan the Republic of Moldova – NATO," a governmental computer emergency response team "Cybersecurity Centre CERT-GOV-MD" was established within the State Enterprise "Centre of Special Telecommunications."[13] The team took responsibility for handling of information security incidents and offering other cybersecurity services to public administration authorities. Given the lack of a national CSIRT and of strong capabilities for cooperation at national and international level, CERT-GOV-MD became the central contact point for cybersecurity incidents in Moldova.

The initiation in 2011 by the Council of Europe of the "CyberCrime@EAP" project gave new impetus to cybersecurity developments in Moldova. The project aimed "to strengthen the capacities of criminal justice authorities of Eastern Partnership countries to cooperate effectively against cybercrime in line with European and international instruments and practices." It envisaged series of seminars, conferences, workshops and training sessions for employees of ministries of justice and the interior, prosecutors' offices, national agencies of public administration and other involved institutions. Planned project results included the identification of strategic priorities regarding cybercrime and electronic evidence, and gaps in existing legislation; judicial and law enforcement trainings; establishing international cooperation among participating institutions.[14]

The implementation of the proposed measures and the support of the "CyberCrime@EAP" project allowed to create in 2012 a Centre for Combatting Cyber Criminality within the General Inspectorate of Police of the Ministry of Interior. The centre took responsibility for activities related to operative investigation, prosecution, international cooperation and identification of persons who commit computer crimes. To accomplish its tasks, the Centre for Combating Cyber Crimes established contacts with subdivisions of the Ministry of Internal Affairs, with other central public administration authorities, local associations, non-governmental organisations, mass media, individuals and businesses, as well as international organisations, including Interpol, Europol, the Southeast European Law Enforcement Centre (SELEC) and the Police Cooperation Convention for Southeast Europe (PCC SEE).

The Centre's establishment by adoption of Law № 66 of 5 April 2012 was followed by amendments to article 134 of the Code of Criminal Procedure of the Republic of Moldova, which allowed competent authorities to perform activities related to the investigation of cybercrimes. These included computer search, rapid preservation of computer data, use of special investigative measures, interception and recording of computer data, monitoring or control access to financial information.[15]

Novelties in Cybersecurity from 2013 - 2015

By 2013, Moldova had achieved significant progress in building information society. The information and communication technologies (ICT) contributed between 8 and 10 % of the gross domestic product. Every second citizen had access to the Internet. More than 50 % of households had at least one computer. The number of students trained in the ICT field significantly increased. However, in spite of large numbers of graduates, most of them did not have adequate practical skills to work in the ICT area due to the lack of qualified teachers, outdated curriculum and educational base. That, coupled with the low level of the population's digital literacy, made public and private sectors easy targets for cyber criminals. Another problem consisted in lacking, among competent bodies, designated by the government coordination centre at national level in relation to cybersecurity. That led to a situation where citizens and businesses were left one to one in the fight against malicious actors. Finally, the emergence of new devices and technologies, and the shift of the paradigm of ICT use dictated new requirements to the information society that, in turn, created a need for the elaboration of a new strategy for its development.[16]

The new strategy, named "National Strategy for Information Society Development – Digital Moldova 2020," and supplement action plan were adopted by government decision No. 857 of 31 October 2013. The strategy aimed at creating favourable conditions for and large-scale use of ICT potential by public institutions, businesses and citizens through minimum state intervention, but with maximum effect. As regards cybersecurity, the strategy envisaged the following: developing Cybersecurity Strategy; training of persons working in the cybersecurity field; raising awareness of risks in the digital space; and developing international cooperation.

According to the action plan, the development of a cybersecurity strategy was assigned to the Intelligence and Security Service (SIS). However, SIS produced a draft strategy without any consultations with stakeholders involved in ensuring cybersecurity and, as of the moment of writing, nothing is known regarding the results of that process.

In 2013, three institutions, namely the Police Academy, the Technical University, and the National Institute of Justice conducted trainings in cybersecurity. However, due to the deficit of instructors and technical capacity, the number of trained people was—and as of 2015 remains—limited, and the knowledge the students obtain during the trainings is still largely theoretical.

To raise awareness and promote cybersecurity among citizens, in 2013 and 2014 the Republic of Moldova joined ENISA's initiative "European Cyber Security Month." Within the frame of the programme two international cybersecurity conferences were held in Moldova. The conferences, organised by CERT-GOV-MD, brought together managers and IT professionals from both the public and private sectors to become aware of emerging cybersecurity threats, trends and possible solutions. However, many individuals and organisations in Moldova still tend to underestimate the danger of the cybersecurity threats and their implications. Thus, CERT-GOV-MD is planning to continue its activity in raising awareness by organising in 2015 a third edition of the international conference.

As the action plan, part of Digital Moldova 2020, did not specifically envisage measures to improve inter-institutional cooperation and solving existing problems in the cybersecurity area, the Office of the Prosecutor General (OPG) took a decision to create a working group, its members being representatives of competent authorities, to facilitate cooperation and strengthen national cybersecurity. To that purpose OPG developed a document called "Joint action plan for preventing and combating cybercrime for the period 2013 – 2015," endorsed by the Office of the Prosecutor General Order No. 60 of 11 September 2013. The plan includes creation of a joint working group to monitor the execution of adopted legislation; creation of CSIRTs within structures responsible for cybersecurity and establishment of a mechanism for cooperation and coordination; organisation of trainings for personnel of law enforcement agencies and specialists in the field of cybersecurity.[17] However, as of 2015, no significant achievements can be reported.

In 2014, the project "Enhancing Cybersecurity: Protecting Information and Communication Networks" was launched, further to recommendations and requirements of the European Cyber Security Strategy, which envisages capacity building and developing of a training program for partner countries. The project aims to build "local capacities to adequately prevent, respond to and prosecute cyber-attacks and/or accidental failures" for Moldova, Macedonia and Kosovo. It is expected that its implementation will lead to creation and development of national CSIRTs and 24/7 contact points, assistance to the development of the national cybersecurity strategy and more effective international cooperation between CSIRTs, law enforcement agencies and the private sector. During 2014 multiple workshops and trainings for institutions dealing with cybersecurity were organised. As of 2015 the project's implementation continues.[18]

Conclusion

Protecting national cyberspace against emerging cyber threats involves a long and complex process of planning and implementing defensive measures, and the Republic of Moldova has gone through a difficult way of putting such measures in place.

The beginning was in 1993 with the adoption of the concept of society informatisation and its implementation. At that time, in spite of the availability of requisite technologies in both public and private sectors, national cyberspace did not exist. Therefore, the main efforts of the state in that and in the subsequent periods were aimed at creating, modernising and developing the main components of the national cyberspace – digital information, information systems and telecommunication infrastructure. The first element of a real national cybersecurity system was installed in 2002 with the creation of the State Enterprise "Centre of Special Telecommunications," which started proving cybersecurity services to state institutions. Later, cybersecurity developments in Moldova were marked by an institutional approach, involving the adoption of a national strategy for the development of the information society and the elaboration of legislative and enforcement measures, which afterwards formed the basis of cybersecurity in the Republic of Moldova. In the following years, amendments were introduced to existing legislation and key laws were elaborated. Though laws were not perfect, their execution, coupled with participation in different international projects, provided impetus for the establishment of specialised cybersecurity and cybercrime units as well as for restructuring the existing ones. Thus, key structures combating cyber threats were created: CERT-GOV-MD, Centre for Combating Cyber Crimes, Division for Cybercrime Investigation and Research, and Department for Combating Cybercrime. By 2013, the new reality and accumulated problems forced a revision of the strategy for development of information society. A new strategy, named "Digital Moldova 2020," changed the methods of ensuring cybersecurity. Since then, persuasion measures have become the main instrument of the state policy in the cybersecurity area.

Based on the historical trajectory of cybersecurity-related developments in Moldova, it could be observed that those have been closely inter-linked with the implementation of the strategies for developing information society. However, in spite of the progress made in the establishment of a legal base, competent authorities and educational institutions, it is too early to speak about existence in the Republic of Moldova of an integrated efficient national mechanism for preventing and combating cybersecurity incidents and cybercrime.

Notes:

[1] Government Decision of the Republic of Moldova No. 155 of 06.03.1995 "On Approval of the Conceptual Design of Information Society in the Republic of Moldova and the Mechanism for Its Implementation."

[2] Government Decision of the Republic of Moldova No. 415 of 05.07.1993, a multi-year development concept, called "The Concept of Society Informatisation and Its Development Mechanism."

[3] UNDP, "National Human Development Report Republic of Moldova," 1995, available at www.md.undp.org/content/dam/moldova/docs/Publications/NHDR/NHDR_1995_english_all.pdf.

[4] UNDP, "National Human Development Report Republic of Moldova," 1998, p. 72, available at www.md.undp.org/content/dam/moldova/docs/Publications/NHDR/NHDR_1998_english_all.pdf.

[5] "Informational System of Public Administration of the Republic of Moldova – "Governmental Intranet," accessed on 30 June 2015, available at http://web.archive.org/web/20020827021747/http://www.ig.moldova.md/en/press-center/30.01.2001/.

[6] Government Decision of the Republic of Moldova No. 735 of 11.06.2002 "On Special Telecommunication Systems of the Republic of Moldova."

[7] Government Decision of the Republic of Moldova No. 255 of 09.03.2005 "On the National Strategy for the Development of Information Society "Electronic Moldova ," accessed on 1 July 2015.

[8] President of the Republic of Moldova Decree No. 1743 of 19.03.2004 "On Building of Information Society in the Republic of Moldova."

[9] Parliament of the Republic of Moldova, Law no. 241 of 15.11.2007 "On Electronic Communications."

[10] "MD CERT in RENAM Network," accessed on 2 July 2015, available at https://www.terena.org/activities/tf-csirt/meeting31/golubev-cert-md.pdf.

[11] Parliament of the Republic of Moldova, Law No. 20 of 03.02.2009 "On Preventing and Combating Cybercrime."

[12] Parliament of the Republic of Moldova, Law No. 278 of 18.12.2008 "For Modification and Completion Criminal Code of the Republic of Moldova."

[13] Government Decision of the Republic of Moldova No. 746 of 2010 "On the approval of the Updated Individual Partnership Action Plan the Republic of Moldova – NATO," accessed on 5 July 2015, available at http://www.mfa.gov.md/img/docs/new_ipap_en.pdf.

[14] Council of Europe, "Assessment Report. Criminal Justice Capacities on Cybercrime and Electronic Evidence in the Eastern Partnership Region," available at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_Project_EaP/Chisinau_International_Conference_Nov2014/CyberEAP%20AssessRep_v15.pdf.

[15] Parliament of the Republic of Moldova, Law No. 66 of 05.04.2012 "For Modification and Completion Criminal Code of the Republic of Moldova."

[16] Government Decision of the Republic of Moldova No. 857 of 31.10.2013 “On the National Strategy for the Development of Information Society “Digital Moldova 2020,” accessed on 6 July 2015, available at mtic.gov.md/en/file/3305/download?token=FiBYBcFg.

[17] Office of the Prosecutor General Order No. 60 of 11.09.2013 “Joint Action Plan for Prevention and Combat with Cybercrime for the Period 2013 – 2015,” accessed on 7 July 2015, available at http://lex.justice.md/viewdoc.php?action=view&view=doc&id=349905.

[18] EU Project “Enhancing Cyber Security,” accessed on July 2015, available at https://www.terena.org/activities/tf-csirt/meeting43/tf-csirt-43-bl.ppsx.

Natalia SPINU is the Head of the Cyber Security Centre CERT-GOV-MD, S.E. Centre for Special Telecommunications, State Chancellery of the Republic of Moldova. She has rich experience in governmental and non-governmental sectors, including previous positions as Department Chief in the State Enterprise “Special Telecommunications Centre” (2008-2009), Lecturer in the Faculty of Economics (2007-2008), Project Coordinator in the Centre of Information and Documentation on NATO, Republic of Moldova (2007). Graduate of the George C. Marshall European Centre for Security Studies, Leaders program in Advanced Security Studies (2012). In 2010, Natalia took part in the three month long European Training Course in Security Policy (ETC) at the Geneva Centre for Security Policy. Master of Arts – Technical University of Moldova, Computer Science (2013-2015), Master of Arts – European Institute of the University of Geneva, Oct 2010-June 2011. She studied Economy, Business and Public Administration (2006-2009), Journalism (2006) and Public Communication (2001-2005) at the State University of Moldova and attended various courses, workshops, conferences, summer schools and seminars organized by academic, governmental or non-governmental institutions in several European countries. Main areas of interest include national and international security, failed states and regional crises.