REGIONAL CYBER SECURITY

The Cases of Georgia, the Czech Republic, Moldova and Serbia

By **POLICE LT. GIORGI TIELIDZE, senior advisor, State Security and Crisis Management Council, Ministry of Internal Affairs of Georgia**

Georgia learned a hard lesson about the need for a national cyber security strategy in 2008, when massive cyber attacks were carried out against national critical informational infrastructure, including the banking sector. The nature of those attacks approached the level of "cyber war" in the sense that the attacks were well-organized attempts to isolate Georgia globally and occurred just as the Russian Federation was engaged in military hostilities against the country.

As a result, the government of Georgia analyzed the grave consequences of that cyber campaign and declared that protecting cyberspace was just as important as protecting the country's sovereignty and territorial integrity.[1] In drafting its National Cyber Security Strategy, the government of Georgia used a slightly different approach from that of Estonia. Unlike Georgia, Estonia had significant cyber security measures in place when the country's networks were simultaneously attacked in 2007, affecting government agencies, banking, media and telecommunications. In retrospect, Estonia was well-prepared for individual cyber attacks but lacked sufficient capacity to counter large-scale and coordinated cyber attacks.[2]

These examples suggest that cyber security is mainly derived from a risk-based approach to information security issues. Governments should first identify and assess their previous experience with information security incidents, risks and challenges to detect possible cyber gaps and vulnerabilities upon which they can focus their specific strategic security visions.

WHAT IS CYBER STRATEGY?

Cyber security strategy and policy establish basic approaches, guiding principles and leading priorities for a nation. These types of documents are general, and their provisions should be reinforced by the passage of specific legal acts (e.g., laws, bylaws, decrees). Cyber security strategies and policies should be formulated systematically to cover a majority of problems and provide adequate countermeasures necessary for addressing those problems. A systematic approach to cyber security strategies and policies should consist of the following pillars:

a) Identifying and analyzing cyber security needs;
b) Defining the capabilities necessary for elimination of cyber security threats;
c) Researching relevant international best practices;
d) Drafting the strategy itself;
e) Devising an action plan that defines the precise measures necessary for executing strategic goals, their timelines, and the governmental agencies responsible for implementing those measures;
f) Carrying out the required measures in practice;
g) Identifying the systems necessary to monitor the progress achieved within the framework of the strategy/policy.

CAPACITIES TO CONFRONT CYBER THREATS

While defining national cyber security strategy, policy planners must identify the available state resources necessary to counter challenges. This step is a prerequisite to identifying relevant strategic priorities and is a cornerstone for all information security strategies and policies. It is pointless to define security measures that cannot be realized with available resources.

When the government of Georgia began drafting its new cyber security strategy, participants of the National Security Council (NSC) Working Group considered the country's limited cyber capacities and decided on a "minimalistic approach" to cyber security. It should be stressed that before the 2008 attacks, Georgia had no experience in building and maintaining effective information security systems. Thus at the initial stage, it was decided to tackle basic problems such as defining minimum information security standards and specifying critical information infrastructure. Policy planners decided not to impose significant financial costs on the public and private sectors, taking into account the development level of the country.

A cyber security strategy working group under the NSC decided upon a Georgian National Cyber Security Strategy that would address basic strategic cyber priorities within two years (2013-2015). Upon completion of these goals, Georgia will shift its cyber policy from a basic approach to a developing model.

RESEARCHING BEST PRACTICES

Cyber security planners should consider international standards and practices while elaborating on relevant strategies. Guidelines provided by world-renowned IT agencies are sufficient, including Microsoft Guidelines for Developing a National Cyber Security Strategy. It is also imperative to research best practices of foreign states that have already fused cyber recommendations into their relevant security policies. Policy planners should ensure that target countries have similar characteristics to their states. It would be useless to follow the examples of states with absolutely different security landscapes, economies and backgrounds.

Georgia's NSC Working Group chose to follow the Estonian example. Both countries are former Soviet republics, have identified similar security concerns, possess limited resources and share a common legacy of defending against massive, coordinated cyber attacks.[3] The NSC also actively cooperated with foreign stakeholders such as Council of Europe (Cybercrime Convention Committee)[4] and the International Telecommunications Union (ITU),[5] which provided feedback and recommendations.

DRAFTING A STRATEGY

Composing the actual strategy is the most important step because it accumulates the results from all the previous stages. A single governmental agency should coordinate the process of elaborating a cyber security strategy. This agency should identify all relevant public and private stakeholders and ensure their participation. The coordinating state body should also divide tasks among other governmental agencies competent in cyber security. Initially, the lead agency should draft a general framework of the strategy and share it with relevant agencies for comment and suggestion. The private sector must be engaged along with the public sector since it, too, owns or operates much of the critical informational infrastructure.[6]

In Georgia, the lead cyber security policy body was the NSC. It coordinated tasks among relevant public institutions (including the Data Exchange Agency, the Ministry of Internal Affairs and the Ministry of Defense) and submitted its draft policy framework to those agencies. Written comments and hearings followed. Furthermore, the NSC Working group actively involved private stakeholders (such as Internet service providers, banking representatives and mobile phone companies). At first, the government of Georgia and ISPs needed to agree on methods of handling cyber incidents consistent with international standards for public-private cooperation. Private stakeholders argued that deep and comprehensive obligatory cooperation would have imposed unjustifiable costs on them and consequently would have hampered cyber-related business development in Georgia. The government concurred, at least temporarily, and agreed to conclude a memorandum of understanding between ISPs and law enforcement agencies that establishes basic principles on cooperation in a manner that wouldn't harm Internet business development in Georgia.[7] Moreover, the NSC held several meetings with civil society representatives to reflect appropriate private interests from human rights perspectives.[8]

ELABORATION OF AN ACTION PLAN

A cyber security strategy without an adequate action plan (AP) cannot be realized. An AP defines precise time frames for achieving priorities and specifies responsible bodies for implementing cyber security measures within those periods.

Policy planners need to assess the operational capacities of the state bodies tasked with carrying out required cyber security measures. Strategists, particularly in developing countries, should not focus on the official functions of public agencies, but rather on the actual assets possessed by them. Those assets include modern technology, qualified staffers and a rich institutional memory.

Furthermore, an AP should establish clear performance indicators, both quantitative and qualitative, to assess when strategic priorities are met. Quite often, APs contain complex activities that necessitate a more detailed approach. In such a case, it's better to write additional ad hoc action plans to avoid overloading the cyber security strategy.

While drafting the Georgian Cyber Security Strategy, the NSC Working Group carefully evaluated the institutional capacities of all governmental stakeholders.[9] It decided that a majority of the AP strategic priorities would be carried out by the Ministry of Internal Affairs of Georgia and the Ministry of Justice Data Exchange Agency, taking into account their relatively advanced experience in informational security.[10]

CARRYING OUT REQUIRED MEASURES

Upon approval of the strategy, implementation begins. Countries in transition should start by adopting a relevant legal framework, which constitutes the foundation for further activities. As soon as laws are passed, institutional changes occur in relevant public agencies, which mean establishing or reorganizing cyber units to correspond to the requirements of the strategy. Along with legal and institutional development, capacity building of relevant cyber security bodies must continue. Improving technology and training is critical to realize strategic priorities.

After the Georgian Cyber Security Strategy was approved by presidential ordinance in May 2013, relevant legislative and institutional changes followed. In November 2013, a list of critical informational infrastructure was designated, for which the state would provide special protection. Furthermore, minimal security standards for critical informational infrastructure were amended as prescribed by the strategy. Moreover, Georgia engaged international partners to help develop cyber capacities operationally.

EFFECTIVE MONITORING

Policy planners should create an effective system for monitoring the progress prescribed by a cyber security strategy, both at the midway point and toward the end. Early monitoring is critical to fulfill cyber security policy requirements since it works as an alarm in case ongoing processes are not working as planned.

More precisely, national security policy bodies should have the capacity to control how relevant stakeholders are performing their duties, offering necessary instructions in case certain agencies fail to meet obligations. Monitors need an operational evaluation system to provide regular status reports on measures and actions.[11]

Georgia pursued such monitoring. All responsible agencies are obliged to report to the NSC Working Group about the latest cyber developments. Based on this information, the NSC provides instructions and schedules for carrying out other activities.

CONCLUSION

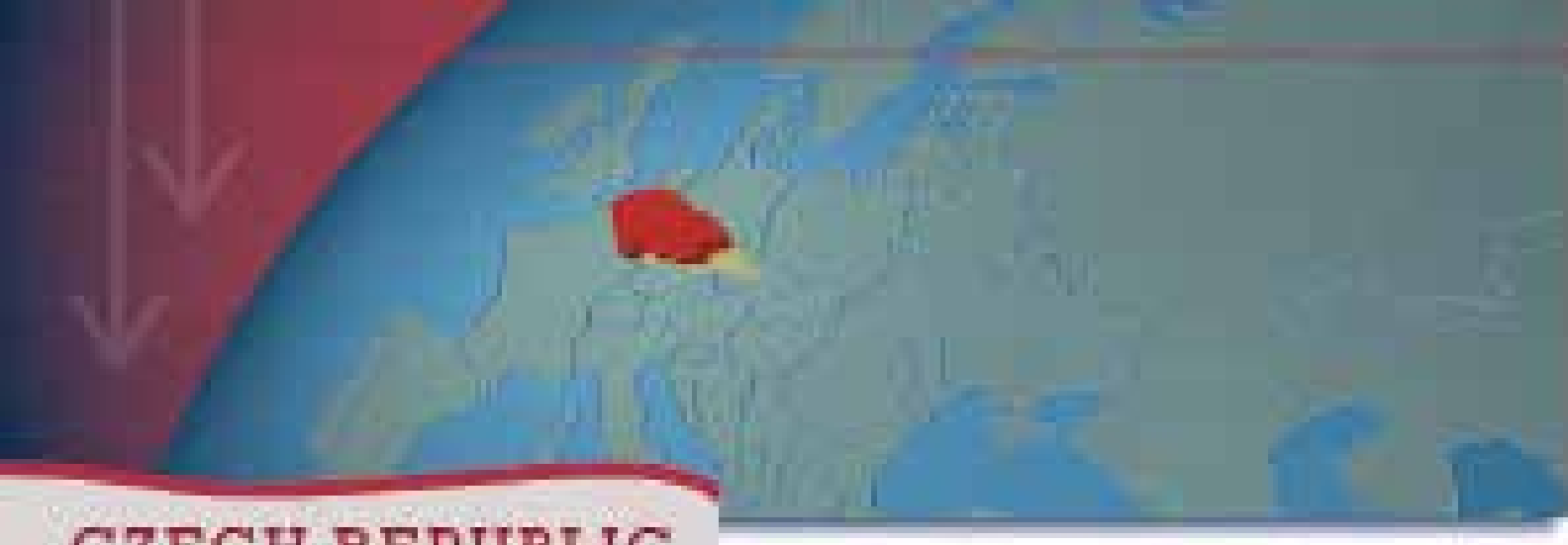
Development of effective cyber security strategies and policies is based on a well-organized elaboration process that should include all the above mentioned stages. All relevant public and private stakeholders should be involved in this process. Cyber security directly affects their legitimate interests as well.

Furthermore, policy planners need to heed international best practices to see if they correspond to the needs of their own country. While establishing the relevance of a foreign state's experience, the following criteria can be used: common legacy, similar economic situation and shared perception of national security threats. At the same time, policy planners should calculate the expense of such strategies to avoid unjustifiable costs to public and private entities.

Finally, the effectiveness of a cyber security strategy depends on its implementation. Implementation should be centrally coordinated and monitored by the highest security policy agency.

CYBER SECURITY STRATEGY AND POLICY ESTABLISH BASIC APPROACHES, GUIDING PRINCIPLES AND LEADING PRIORITIES FOR A NATION.

1. Cyber Security Strategy of Georgia for 2013-2015, p. 2 (available in Georgian only) accessed on January 17, 2014: http://www.nsc.gov.ge/files/files/legislations/kanonqvem-debare%20normatiuli%20aqtebi/cyber%20security%2017%20may.pdf
2. Cyber Security Strategy of Estonia, p. 6, accessed on January 19, 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Estonia_Cyber_security_Strategy.pdf
3. e.g Georgian and Estonian National Security Strategies and Cyber Security Strategies.
4. Regional Seminar on Strategic Cybercrime Priorities, Council of Europe Cybercrime Convention Committee; accessed on January 17, 2014: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_Project_EaP/2523_Strategic%20Priorities_Tbilisi_V4_19june12FIN.pdf
5. ITU Cybersecurity Mission to Georgia, p. 14-16, International Telecommunication Union; accessed on January 17, 2014: http://www.itu.int/ITU-D/cyb/app/docs/Salta_101101/Session4/Probert_Presentation.pdf
6. Developing a National Strategy for Cybersecurity, p.17 Microsoft Corporation, accessed on January 17, 2014: http://download.microsoft.com/download/B/F/0/BF05DA49-7127-4C05-BFE8-0063DAB88F72/Developing_a_National_Strategy_for_Cybersecurity.pdf
7. Codexter Cyber Terrorism Country Profile – Georgia, p. 5; accessed on January 17, 2014: http://www.coe.int/t/dlapil/codexter/Source/cyberterrorism/Georgia.pdf
8. Office of NSC Presents Draft Cyber Security Strategy for Public; Official Webpage of the National Security Council of Georgia, accessed on January 17, 2014: http://www.nsc.gov.ge/eng/news.php?id=6170
9. ENISA National Security Strategies – Practical Guide on Development and Execution, p. 31; accessed on January 17, 2014: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide
10. See Action Plan of the Cyber Security Strategy of Georgia.
11. Supra, ENISA National Security Strategies p.18.



By DANIEL BAGGE
National Cyber Security Center, Czech Republic

Ensuring the cyber security of a state is one of the key challenges of our times. The absence of geographic and physical limitations in cyberspace is the driving force behind the need for a new approach toward security. Although the cyber domain complements other domains, such as air, sea, land and space, it is also a domain in itself. Within this new domain, we cannot rely on capacities designed for better-known domains. The omnipresence of cyber threats requires intense international cooperation based on the composition of current international bodies. Nations must adopt new approaches, forge new partnerships and broaden cooperation among institutions. We must dispose of the security toolbox we used in the past: Bullets and guns are useless in the face of a cyber threat.

To forge new partnerships internationally, share capabilities and enhance security cooperation, an entirely new and comprehensive approach toward cyber security must be adopted at the national level. Only through a well-designed and whole-of-government approach can a viable model be built to promote cyber security and enhance national security. The main task for every state is to create a cyber security environment based on technical and theoretical capabilities, a legal framework and interagency cooperation.

This article presents the steps taken by the Czech government and security entities to advance cyber security nationally, regionally and internationally. The Czech Republic, as a medium-size Central European country, has an obligation to protect its citizens and secure cyberspace to allow the free exchange of information and undisrupted flow of information and commerce. The state must also protect critical infrastructure vital not only to itself, but to its neighbors, for example, in the energy sector. Also, as a member of the European Union and NATO, we have obligations to our allies and partners to enhance cyber security internationally.

NATIONAL CYBER SECURITY CENTRE

Cyber security is part of the Czech Republic's security environment. Cyber attacks are becoming more sophisticated, dynamic and complex. No longer is the Internet used merely by criminals for their direct economic benefit. The sphere of attacks has widened to include industrial espionage, cyber terrorism and vandalism and probing critical infrastructure. Attackers concentrate increasingly on elements of critical infrastructure, such as power plants, pipelines, intellectual property and health care information systems.

Aware of the growing scale of cyber threats to national security, the Czech government announced the creation of the National Cyber Security Centre (NCSC) within the National Security Authority on October 19, 2011.

The NCSC establishes the foundation for a coordinated whole-of-government approach and aims to bring all cyber security-related policies under one roof. It is responsible for national security in the cyber domain, critical infrastructure protection, legislative measures concerning cyber security, international cooperation, a Computer Emergency Response Team (CERT) and setting standards. The NCSC is not a law enforcement agency, so cyber crime is not the primary agenda; however, cooperation with law enforcement and the intelligence community is one of its roles.

LEGAL FRAMEWORK

Ensuring that the entire cyber domain follows the technical guidance of the NCSC required new legislation. The first step is defining critical infrastructure. It includes not only government networks, but private telecommunication networks and information systems and the industrial control systems of dams, power plants and other vital industrial and economically important sectors.

Efforts to adopt a legislative act were framed by consultations with an interagency working group consisting of representatives from the Ministry of Interior, Ministry of Defense, the Czech Telecommunications Office, the General Directorate of the Fire Rescue Service and intelligence services. The law sets out certain obligations, depending on whether the subject is critical or important, and gives the NCSC authority to inspect whether obligations are fulfilled.

NATIONAL COOPERATION

The second platform vital for a viable cyber security strategy is national cooperation, and is sometimes referred to as interagency cooperation. In fact, these two terms are not exact. The first refers to a mindset and an NCSC-centric approach. The governing body sets standards and campaigns for cooperation from entities involved in cyber security. Interagency cooperation is more horizontal, as other agencies and entities complement one another's efforts.

For example, national cooperation could mean a government agency follows NCSC guidelines, but interagency cooperation could mean the NCSC provides the agency with valuable intelligence about attempted cyber intrusions.

INTERNATIONAL COOPERATION

Cyberspace has no geographical borders or limitations. That fact increases the importance of international cooperation. The chronic lack of attribution in the cyber domain calls for strong cooperation among allies and the creation of new partnerships. Cyber is not just a domain that expands the existing area of potential conflict and allows hacktivists, organized crime and terrorist networks to thrive. Cyber is not just a digital highway used for attacks. It also is a means for criminals to launder money and exchange tactics. Also, the computerized interdependency between industry and consumers constitutes the battlefield of industrial and political espionage against the interests of your country.

All these threats cannot be handled by only one security entity. The very foundations of the cyber realm call for enhancing bilateral and multilateral cooperation at the agency, national and international level. Cooperation does not mean only the exchange of technical expertise but also shaping policies, creating awareness and coordinating efforts. Training programs and exchange of best practices among policy makers, politicians and government officers are essential for mutual understanding. Without agreement on basic terms and definitions, it is impossible to seek common goals.

Once international cooperation is established with neighboring countries and international partners, the security entity must not falsely assume its job is complete. Simulations and exercises among technical and decision-making bodies should be routine, and policies should be updated by the exchange of expertise and training methods.

One often overlooked way of improving cyber security is promoting "digital hygiene": educational campaigns to inform the public about threats and best practices in cyberspace. Breaches in security often begin between the keyboard and the chair. These campaigns can also be developed in collaboration with international partners, such as the European Union Agency for Network and Information Security or the Organization for Security and Co-operation in Europe.

SIX PRIORITIES

The Czech NCSC has established six cyber security priorities. They start with legislation to create a legal framework that defines the competence of public authorities and the rights and obligations of operators in the cyber security field.

International cooperation and communication is the second priority. Preparedness exercises and simulations should be organized nationally and internationally with multinational partners. Some of these events should include private-sector actors endangered by cyber threats.

A third priority is national cooperation: Large-scale interagency cooperation, as well as cooperation between public and private sectors, is vital. At the same time, cooperation with academia and outside experts should be established to develop cyber security capabilities.

Mapping out the risk to critical information infrastructure represents the fourth priority. Mapping helps raise awareness about the growing number of systems that can become cyber targets. An analysis evaluates the importance and significance of such systems, as well as their role within the functioning of the state. Risk assessment then helps minimize damage after a potential incident and set up key systems' protection for maintaining cyber security.

A fifth priority is building a specialized workplace for NCSC/CERT. NCSC is supposed to build and maintain a mutual early warning system, as well as connect this system into already existing international early warning systems for cyber threats. The CERT is tasked with monitoring cyberspace and detecting attacks. Such a workplace is highly skilled and fully integrated with similar institutions outside the Czech Republic.

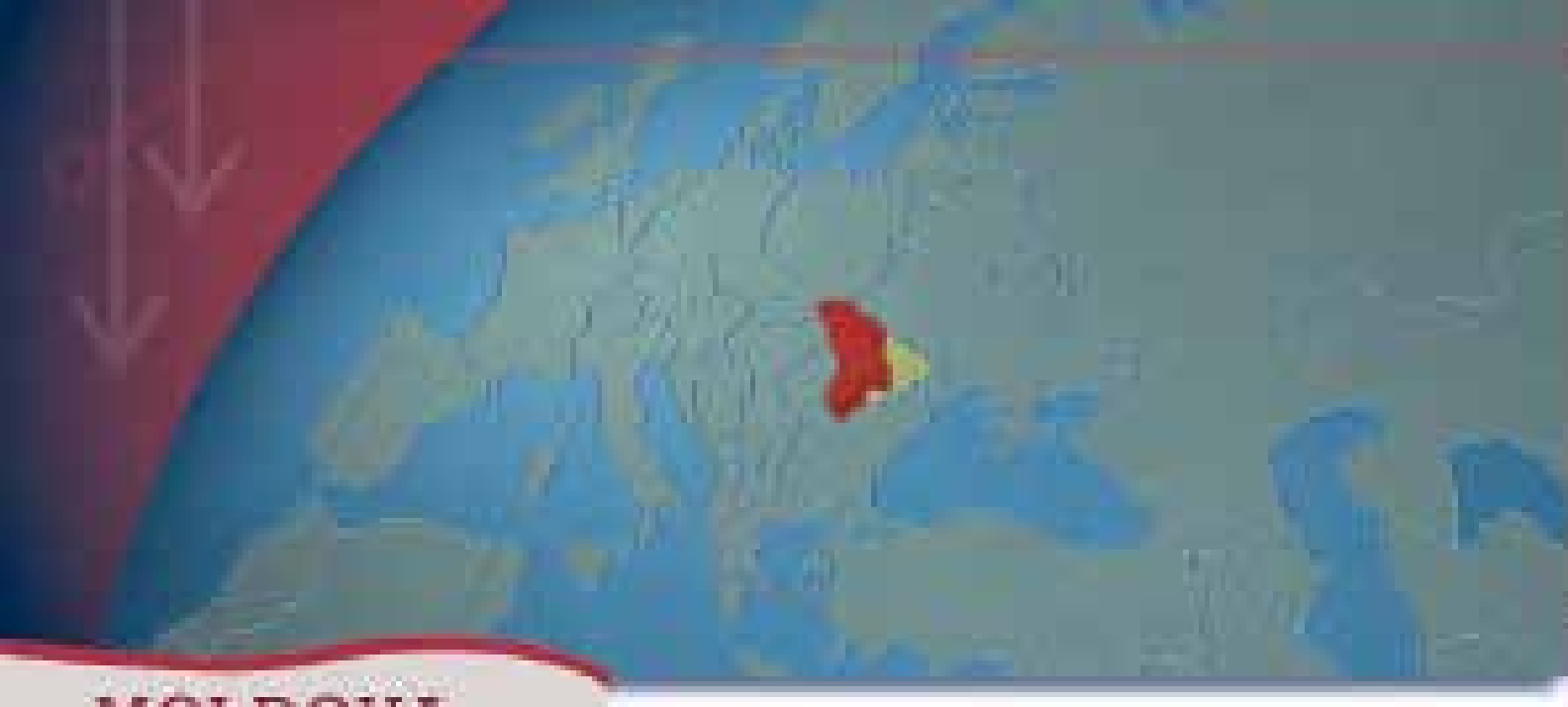
A final priority is raising cyber security awareness, not just among leaders and specialists, but also the public at large.

CONCLUSION

The Czech Republic recognizes the complexity of cyber threats and is adopting measures to ensure cyber security in three layers — critical infrastructure, governmental networks and public computers. To reach all three layers, a whole-of-government approach is necessary, combined with cooperation from the private sector and the public.

Isolated efforts that fail to achieve all of the six priorities won't accomplish the strategic goal of securing cyberspace. Only combined and coordinated efforts will create a comprehensive cyber security framework that protects the Czech Republic and its international partners.

CYBER SECURITY IS PART OF THE CZECH REPUBLIC'S SECURITY ENVIRONMENT.



By **NATALIA SPINU**
Head of the Cyber Security Center
CERT-GOV-MD, Republic of Moldova

Today, cyber security is one of the world's most widely discussed topics, capturing the attention of national leaders at the majority of international security events. Consisting of a multitude of actions and controls, cyber security is seen as the guarantee of national, economic and even personal security. The Internet and information technology are transforming the global economy and creating new opportunities for society and government. Moldova's citizens, businesses and government are readily embracing the many advantages that these technologies offer.

The IT business revolution has resulted in traditional services increasingly becoming available online. In the name of convenience, everyday activities such as banking, shopping and accessing government services are taking place online. In keeping with this trend, Moldova's government and private sector are using the Internet and other digital technology to facilitate interaction with citizens.

Almost half of Moldovans are already online (38 percent have broadband access), and they expect online public services to be accessible 24 hours a day, seven days week, through their computers or mobile phones. But the increased use of the Internet and other digital technology increases our vulnerability to cyber threats. Criminals are using cyberspace to gain access to personal information, steal intellectual property from businesses and gain knowledge of sensitive government-held information for financial or political gain, or other malicious purposes. In the cyber world, national borders present no barrier.

As an example of how cyber security is being acknowledged and developed in a state, I would like to present the example of the Republic of Moldova, a onetime republic of the former Soviet Union. Moldova is deeply involved in various national and international projects and initiatives to create a safe and secure system for all. Since cyber security is borderless, it can be achieved only through cooperation and collaboration among states.

CYBER SECURITY HAS NO BORDERS

A successful targeted cyber attack could disrupt a state's critical services, harm the economy and potentially threaten national security. Moldova is not immune from such attacks. For example, in the last quarter of 2013, more than 10,000 attacks targeted government computers. It is unclear whether these attacks were attempted by individuals using specialized tools or by criminal organizations. Fortunately, these incursions were detected and the nefarious activity blocked. Moldova is also facing cyber threats to its critical information infrastructure. Given the interdependence of information infrastructure and sectors such as banking, transport, energy, social welfare and national defense, this is a cause for concern.

Moldova's government acknowledges the need to improve cyber security and understands that such security is directly correlated to national security in this technology-globalized era. The completion of national legislation in this area, including the establishment and enforcement of baseline security measures for national information infrastructure, is a government priority. This is one of the main pillars of a cyber security system.

CYBER CHALLENGES

One of the main disadvantages of the digital era is its dependence on systems and networks. Security issues are omnipresent. When it comes to cyber security, we acknowledge

that it is important for citizens to have confidence in state and private institutions. Therefore, Moldova's cyber security response must meet the challenging nature of growing and evolving cyber threats.

In 2010, Moldova launched the Governance e-Transformation process. This strategic program provides a unified vision to modernize and improve the efficiency of public services through IT governance. Information assurance — confidence in the security, integrity and availability of information systems — is therefore essential. A logical development would include implementing new systems, together with new protection measures. The fast-paced development process in the last decade unfortunately did not include enough controls to assure comprehensive cyber security.

MOLDOVA IS DEEPLY INVOLVED IN VARIOUS NATIONAL AND INTERNATIONAL PROJECTS AND INITIATIVES TO CREATE A SAFE AND SECURE SYSTEM FOR ALL.

Moldova is not alone in facing these challenges: It is inextricably linked with global IT development and emerging cyber threats.

Keeping information assets secure in today's interconnected computing environment is a challenge that becomes more difficult with each new "e" product and each new intruder tool. There is no single solution for securing information assets; instead, a comprehensive approach ensuring a multilayered security strategy and policies is required. One of the layers that governments are including in their strategies today is a computer security incident response team.

CERT-GOV-MD

Prevention, protection and detection methods must properly address existing risks. The lack of a security culture is one the biggest challenges for decision-makers and users. Developing and implementing a comprehensive set of minimum requirements across the whole of government and society is necessary to ensure cyber security. Even small changes to education, procedures and policy can raise the overall security level.

At the government level, several initiatives came to life. One of these is the establishment of a Computer Emergency Response Team, known as Cyber Security Center CERT-GOV-MD, created in partnership with NATO as a part of the Center for Special Telecommunications in the State Chancellery. CERT-GOV-MD will build on existing technical, cyber security and information assurance capabilities of the Center of Special Telecommunications to provide continuous protection of government systems and information against advanced and persistent threats.

CERT-GOV-MD is a unique entity for national data systems and public authorities. CERT-GOV-MD receives and processes information on existing or potential cyber threats, offers recommendations on the safe use of online data and provides assistance to Moldova's public administration in preventing and mitigating cyber incidents. Cooperating with various institutions, both national and international, CERT-GOV-MD is fully functional.

Still, the human factor is always the weakest link in the system. It is encouraging that in many countries IT security is a mandatory part of education. Young specialists are aware of new technologies and risks associated with IT and, therefore, it is the new generation that tends to drive necessary change. Moldova is striving for such educational upgrades. One of the action plans suggests creating minimum cyber security training and education requirements for public servants. This is very challenging, because the different age groups are prone to look at this issue differently. Also, changes have to be made incrementally to improve long-term retention. Cooperative international action and the sharing of best practices would improve cyber security for everyone.

The plans listed above are part of a complex strategy. The creation of CERT-GOV-MD, as well as practical training and legislative initiatives, are steps Moldova is taking to address threats. It's encouraging that in the few years since the creation of CERT-GOV-MD, the number of projects per year and people involved rise continuously. The effects of this cooperative effort across the whole of government are positive and provide tangible results by improving cyber security for everyone.

CONCLUSION

As cyber attacks grow in number and sophistication, the threat is viewed as a problem in both national and international security contexts. Yet assessments of how real the threats are, where the dangers lie, who is best suited to respond to them, and what kind of international measures and strategies are appropriate to protect information societies from malicious actors — in short, how best to safeguard long-term stability and peaceful use of cyberspace — vary widely.

The evolution of cyber threats means it is imperative that security is placed at the forefront of any organization. Unfortunately, individuals and organizations tend to underestimate the scope of the cyber security threat. It is important to enhance a public-private-civilian dialogue that will likely offer ideas and options to identify technical and policy solutions for building resilience in information systems. The Moldovan government is ultimately responsible for protecting its own systems and helping critical national infrastructure providers ensure its citizens can access government and other essential services. By becoming a leader in cyber security, Moldova can be a trendsetter in the digital world.

By **ZVONIMIR IVANOVIĆ**
University of Criminalistics and Police Studies, Belgrade

Modern innovations in communications technology have changed the world, but the same technology that has made modern society more productive has also been exploited by terrorists and criminals, creating new security and law enforcement challenges. As Serbia has transitioned into a 21st-century European democracy, it has strived to reform its legal system and law enforcement structures to manage the challenges presented by modern cyber crime.

Following the breakup of Yugoslavia, Serbia faced practical problems — a period of meandering legal theory and faltering reforms — but has finally achieved its goals. First, it is necessary to point out some irregularities in the Serbian legal system. Although Serbia has ratified certain Council of Europe Conventions,[1] no existing law adequately covers cyber crime with regard to information and communications technology (ICT). However, many secondary laws regulate certain aspects in detail. The responsibilities of some government agencies and ministries to enforce cyber crime laws do not correspond with their powers, and the partitioning of the Serbian legal system creates difficulties for those who must enforce the laws.

In July 2005, a law was passed creating a special prosecutor's office for cyber crime within the Office of the High Prosecutor, and establishing a special council of the court under the jurisdiction of the High Court of Belgrade.

But the Serbian legal system did not cover ICT and cyber crime until 2006, when it became necessary under obligations of the Cybercrime Convention of the Council of Europe (CETS 185). Although the former Union of Serbia and Montenegro signed CETS 185 (and the following protocol, CETS 189) in 2005, Serbian legislation did not cover cyber crime until the following year, when it was only partially covered by the Serbian Criminal Code.[2] Since then, the Serbian legal system has been frequently and thoroughly modified, a process to which a working group — formed under CETS 185 and 189 and implemented as part of the Council of Europe led Cybercrime@IPA SEE[3] project — contributed greatly.

In 2008, the High-Tech Crime Unit (HTCU), a special department for combating cyber crime, was established within the Ministry of Internal Affairs' Service for Combating Organized Crime. The HTCU is composed of two sections — a section for combating electronic crime and a section for combating intellectual property crime (copyright infringement and forgery). The HTCU has jurisdiction over pretrial proceedings for criminal acts involving cyber crime and crimes executed using computers and computer networks.

The Ministry of Internal Affairs is responsible for investigating (under the public prosecutor) criminal acts involving distribution of illegal content on the Internet and infringement of intellectual property rights. The HTCU can conduct investigations into crimes against computer systems as well as all crimes that involve technology. Digital forensics collection and analysis is not conducted by the HTCU, but entrusted to special services under the Ministry of Internal Affairs.

HTCU cooperates with foreign cyber crime

specialists via direct officer-to-officer communication through various international police organizations, such as Europol and Interpol and the Southeast European Law Enforcement Center, and through 24/7 networks and points of contact established by CETS 185.

Changes in the criminal code[4] in August 2009 made the Serbian legal system more, but not fully,[5] compliant with CETS 185 and 189.

A law on the organization and jurisdiction of government agencies in combating cyber crime[6] was passed in December 2009 to delineate jurisdictional responsibilities in cyber crime enforcement. Article 3 states that it governs investigation, indictment and prosecution of criminal acts such as: breaching computer data security; computerized offenses against intellectual and physical property and commerce; and offenses against human rights, including child pornography.

TRACKING ILLICIT MONEY

The law on the confiscation of property of criminal offenders has general provisions designed to stop the flow of illicit money and to search for, seize and confiscate criminal proceeds. It is possible to conduct a financial investigation and confiscate assets, regardless of the type of crime.

POLICE ACTIONS

To initiate criminal proceedings, evidence of a crime is required. As part of a criminal investigation, police officers conduct searches to collect evidence and other physical items or information useful for criminal proceedings, or to apprehend or prevent the escape of suspected perpetrators.[7]

The Law on Special Measures for the Prevention of Criminal Offenses Against the Sexual Freedom of Minors (Mary's Law) prescribes special measures for those who sexually abuse children and governs record keeping of people convicted of these crimes.[8] It includes stipulations on sexual abuse of minors through cyber crime. It also commissions government agencies within the Ministry of Justice to enforce criminal sanctions to include tracking, informing of movement, and storing sexual offender records.

CONCLUSION

Serbia's approach to cyber crime is scientifically and practically founded. Serbia has learned from its mistakes in this strategically important field. The path was very difficult but also fruitful. The Serbian legal system has experienced minor strains, but now has taken solid procedural,

THERE IS NO PERFECT SYSTEM, BUT SERBIA'S HOLISTIC APPROACH REPRESENTS A GOOD START AND IS PROVIDING RESULTS.

If an offense was committed using the Internet and meets these general provisions, a financial investigation will be conducted as well. The prosecutor initiates such an investigation, which is conducted by the Financial Investigation Unit (FIU) in the Ministry of Internal Affairs. Institutional roles are as follows:

- Ministry of Finance – Administration for the Prevention of Money Laundering collects and analyzes data on suspicious transactions;
- Ministry of Internal Affairs – The FIU conducts investigations to identify and locate assets obtained through crime;
- Ministry of Justice – The Department for Organized Financial Crime leads pretrial proceedings to identify cyber crime and other offenses carried out using computers and computer networks, prosecutes offenders, conducts court proceedings, and manages seized property.

organizational and functional measures to meet the challenges posed by cyber crime. There is no perfect system, but Serbia's holistic approach represents a good start and is providing results.

Creating and managing this system is not possible without the help of international partners, and their efforts are acknowledged. All parts of the system were built to develop capacities to answer the challenges of new technologies and their misuse in the form of cyber crime. □

1. Before all Council of Europe Conventions – CETS: No. 185. and No.189.
2. Official Messenger of the Republic of Serbia no. 85/2005.
3. Official information about the project can be found at: http://search.yahoo.com/r/_ylt=A0oG7nw5J9lSQmMAEfpXNyoA;_ylu=X3oDMTBybnZlZnRlBHNlYwNzcgRwb3MDMQRjb2xvA2FjMgR2dGlkAw--/SIG=14s71c2eq/EXP=1389991865/**http%3a//www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%2520project%2520balkan/Mar11_Belgrade_Money_flows/Belgrade_A.Seger.pdf, last accessed January 17, 2014.
4. Official Messenger of the Republic of Serbia, no. 72/2009.
5. This means that there are still some inconsistences' regarding implementation of Cybercrime Convention.
6. Official Messenger of the Republic of Serbia, no.104/09.
7. Ivanović, Z. and Žarković, M. "Scientific approach to building teams for seizure of digital evidence," pp. 399-413 in Thematic proceedings of international significance, Vol I, Academy of Criminalistics and Police Studies, 2013, Ed. Goran Milošević, p.400.
8. Official Messenger of the Republic of Serbia, no. 32/13.