CYBERSPACE RISKS AND THREATS TO CRITICAL INFORMATION INFRASTRUCTURE

Major General (ret) Professor Constantin MINCU, PhD [*]
Colonel (ret) Professor Gruia TIMOFTE, PhD [**]

Critical infrastructures are those physical and cyber-based systems essential to the minimal economy and government operations. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. Many of the national critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of progress in communication and information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. The same progress has created new vulnerabilities to equipment failure, human error, weather and other natural causes, physical and cyber attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and the private sectors, and protect both domestic and international security.

Keywords*: cyberspace, critical information infrastructure, communication and information technology, cyber vulnerability, threat and risk, cyber security.*

Critical infrastructures are systems and assets, whether physical or virtual, so vital to nations that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of the aforementioned sectors. The critical infrastructure sectors are: agriculture and food, banking and finance, chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, government facilities, information technology, national monuments and icons,

[*] Full member of the Romanian Scientists' Academy, scientific secretary of the Military Sciences Section, member of the Romanian Scientists' Academy Honor Council (mincu_constantin@yahoo.com)
[**] gruia.timofte@gmail.com

nuclear reactors, materials and waste, post and shipping, public health and health care, transportation systems, and water.

Addressing these threats depends on effective partnerships between the government and private sector owners and operators of the critical infrastructure. Therefore, it is necessary to have a partnership model that includes public and private councils to coordinate policy and information sharing, as well as analysis centers to gather and disseminate information on threats to the physical and cyber-related infrastructure.

Recent cyber attacks on corporations from different countries highlight the threats posed by the worldwide connection of the networks. Since the private sector owns most of the nations' critical infrastructure – such as banking and financial institutions, telecommunications networks, and energy production and transmission facilities - it is vital that the public and private sectors form effective partnerships to successfully protect these cyber-reliant critical assets from a multitude of threats including terrorists, criminals, and hostile nations [1].

National policy must establish various mechanisms for the development of public-private partnerships. The councils create the structure through which representative groups from all levels of government and the private sector are to co-operate in planning and implementing efforts to protect the critical infrastructure. The sector councils are conceived so as to be policy-related and to represent a primary point of contact for the government in planning the entire range of infrastructure protection activities, including those associated with mitigating cyber threats. Their objectives are to determine (1) the private sector stakeholders' expectations for cyber-related, public-private partnerships and to what extent these expectations are being met and (2) the public sector stakeholders' expectations for cyber-related, public-private partnerships and to what extent these expectations are being met. Public and private organizations rely on computer systems for transferring increasing amounts of money; sensitive proprietary economic and commercial information; classified and sensitive non-classified defense and intelligence information. The increased transfer of critical information heightens the risk that malevolent individuals may attempt to disrupt or disable the national critical infrastructures and obtain sensitive and critical information for malicious purposes. To address the threats to the nation's cyber-reliant critical infrastructure, national policy needs to emphasize the importance of public-private coordination.

1.Cyber Threats to the National Critical Infrastructure

Different types of cyber threats from numerous sources may adversely affect computers, software, a network, an agency's operations, an industry, or the Internet itself. The global interconnectivity provided by the Internet allows cyber attackers to easily cross national borders, to access a vast number of victims at the same time, and to easily maintain anonymity. Cyber threats can be unintentional or intentional. Unintentional threats can be caused by software upgrades or maintenance procedures that inadvertently disrupt

systems. Intentional threats include both targeted and untargeted attacks. Attacks can come from a variety of sources, including criminal groups, hackers and terrorists. The main sources of threats that have been identified by the intelligence communities and others are as follows:

- **Bot-net operators** use a network, or bot-net, of compromised, remotely controlled systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial of service attack or servers to relay spam or phishing attacks).
- **Criminal groups** seek to attack systems for monetary gain. Specifically, organized criminal groups use spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and criminal organizations also pose a threat to other countries through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
- **Hackers** break into networks for the thrill of the challenge, bragging rights within the hacker community, revenge, stalking others, and monetary gain, among other reasons. While gaining unauthorized access once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use.
- **Insiders** are the principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access so as to cause damage to the system or to steal system data. The insider threat includes contractors hired by the organization as well as employees who accidentally introduce malware into systems.
- **Nations** use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications and economic infrastructures that support the military power of other countries.
- **Phishers** are individuals or small groups that execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.
- **Spammers** are individuals or organizations that distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware or attack organizations (i.e., denial of service).
- **Spyware/malware** authors are individuals or organizations with malicious intent that carry out attacks against users by producing and distributing spyware and malware.

▪**Terrorists** seek to destroy, incapacitate or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

Groups or individuals may intentionally deploy cyber exploits targeting a specific cyber asset or attack through the Internet using a virus, worm or malware with no specific target. The main types of cyber exploits are as follows:

•**Denial-of-service** is a method of attack from a single source that denies system access to legitimate users by overwhelming the target computer with messages and blocking legitimate traffic. It can prevent a system from being able to exchange data with other systems or use the Internet.

•**Distributed denial-of-service** is a variant of the denial-of-service attack that uses a coordinated attack from a distributed system of computers rather than from a single source. It often makes use of worms to spread to multiple computers that can then attack the target.

•**Exploit tools** are publicly available and sophisticated tools that intruders of various skill levels can use to determine vulnerabilities and gain entry into targeted systems.

•**Logic bombs** are forms of sabotage in which a programmer inserts codes that cause the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment.

•**Phishing** represents the creation and use of e-mails and Web sites- designed to look like those of well-known legitimate businesses, financial institutions, and government agencies - in order to deceive the Internet users into disclosing their personal data, such as bank and financial account information and passwords. The phishers then use that information for criminal purposes, such as identity theft and fraud.

•**Sniffer** is a program that intercepts routed data and examines each packet in search of specific information, such as passwords transmitted in clear text.

•**Trojan horse** is a computer program that conceals a harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute.

•**Virus** is a program that infects computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate.

•**Vishing** is a method of phishing based on Voice-over-Internet-Protocol technology and open-source call center software that have made it inexpensive for scammers to set up phony call centers and for criminals to send e-mail or text messages to potential victims, saying there has been a security problem, so they need to call their bank to reactivate a credit or debit card, or send text messages to cell phones, instructing potential victims to contact fake online banks to renew their accounts.

•**War driving** is a method of gaining entry into wireless computer networks using a laptop, antennas, and a wireless network adapter that involves patrolling locations to gain unauthorized access.

•**Worm** is an independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.

•**Zero-day exploit** is a cyber threat taking advantage of security vulnerability on the same day that the vulnerability becomes known to the general public and for which there are no available fixes.

Recent reports of cyber attacks illustrate that such attacks could have a debilitating impact on national and economic security and on public health and safety.

In May 2007, Estonia was the reported target of a denial-of-service cyber attack with national consequences. The coordinated attack created mass outages of its government and commercial Web sites [2].

In March 2008, U.S. DoD reported that in 2007 computer networks operated by DoD, other federal agencies, and defense-related think tanks and contractors were the targets of computer network intrusions. Although those responsible were not definitely identified, the attacks appeared to have originated in China [3].

In January 2010, it was reported that at least 30 technology companies - most of them from Silicon Valley, California - were victims of intrusions. The cyber attackers infected the computers with hidden programs allowing unauthorized access to files that may have included the companies' computer security systems, crucial corporate data, and software source codes [4].

In January 2010, a California-based company filed suit alleging that two Chinese companies stole a software code and then distributed it to tens of millions of end users as part of the Chinese government-sponsored filtering software. The company claims more than $2.2 billion dollars. Academic researchers found that portions of the company's software code had been copied and used in initial versions of the Chinese software [5].

Based on an 8-month investigation in 2009, university researchers reported that the computer systems in India were attacked. The suspected cyber attackers got remotely connected to Indian computers using social networks to install bot-nets that infiltrated and infected the Indian computers with malware. The incidents were reported to have been traced back to an underground espionage organization that was able to steal sensitive national security and defense information [6].

Using the partnership program between the private and the public sectors coordinates them so as to manage the risks related to critical cyber information infrastructure protection. This coordination includes sharing information, conducting exercises and providing resources.

Sharing information. Information sharing enables both government and private sector partners to assess events accurately, formulate risk assessments and determine appropriate courses of action. This includes sharing information on cyber threats and vulnerabilities, providing alerts or warnings about such threats and recommending mitigation steps.

Conducting exercises. Building and maintaining organizational and sector expertise requires comprehensive exercises to test the interaction between or among stakeholders in the context of serious cyber attacks, terrorist incidents, natural disasters and other emergencies. Exercises are conducted by private sector owners and operators, and across all levels of government.

Providing resources. Maximizing the efficient use of resources is a key element in protecting the national critical infrastructure. This includes technical and policy expertise, training, commitment of people and financial aid through grants.

2. Cyber Security Requirements of the Critical Infrastructure Sectors

a. Threats, vulnerabilities, incidents and the consequences of potential attacks are increasing. Critical infrastructures can be threatened by both physical and cyber means. Several organizations and individuals are capable of conducting such attacks. However, with the critical infrastructures' increasing reliance on computers and communications networks, more organizations and individuals can cause harm by means of cyber attacks [7].

b. Critical infrastructure sectors face various cyber threats. In addition to posing these physical threats, terrorists and other persons/groups with malicious intent, such as transnational criminals and foreign intelligence services, pose a threat to our nation's computer systems. The officials are increasingly concerned about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, etc.

c. Poor system management can be costly and disruptive. This category may include mundane cyber security threats such as: inadequate system monitoring and control tools; unplanned growth of a large, complex system with external interdependencies; a combination of seemingly unlikely external factors; lack of a well-defined stakeholder responsible for overall robustness; operator confusion and mistakes. These threats receive little attention and yet they emerge as a serious risk to national economic growth and to the success of several government and private sector initiatives. These activities ascribe critical roles to computer-operated systems in relation to the economy, government, military or nationally important industry sectors. The systems are growing through an unplanned, organic process of accretion, without any sort of global plan and without a well-defined entity with clear responsibility for security and reliability. The resulting systems are intrinsically hard to analyze or monitor, so that even if the nation were to mandate that they be controlled, the science for doing so would often be lacking.

d. Growing concern over connections between cyber and physical worlds. For instance, a cyber attack that disables the water supply or the electrical system, in conjunction with a physical attack, could deny emergency services the necessary resources to manage the consequences of the physical attack, such as controlling fires, coordinating actions, and generating light.

e. Critical infrastructures rely on information technology to operate. Entities within each of the critical infrastructure sectors rely on similar types of information technology to perform both critical and non-critical functions, such as accounting, finance, personnel, manufacturing, engineering and logistics, which are essential in fulfilling their missions, such as generating and transmitting electric power, providing water, making chemicals, transporting goods and people or supporting financial transactions.

Because infrastructure sectors make use of similar computer and network technologies, they have similar needs for cyber security. However, the level of importance placed on various aspects of cyber security varies. For instance, cyber security requirements are often described in terms of the confidentiality, integrity or availability of data and systems. Confidentiality ensures the preservation of authorized restrictions on the access and disclosure of information, including means for protecting personal privacy and proprietary information. Integrity is defined as guarding against the improper modification or destruction of information, and includes information non-repudiation and authenticity. Availability means ensuring timely and reliable access to and use of information.

3. Cyber Security Technologies and Standards

Critical infrastructure owners use current cyber security technologies, such as firewalls and antivirus software, to help protect the information that is processed, stored, and transmitted in the network systems that are prevalent in the infrastructures.1 To help infrastructure owners purchase cyber security technologies, standards are available that describe the operating characteristics and qualities of cyber security technology products. Standards that describe protocols and operating guidelines that describe how to use technology products are also available [8].

a. The following categories of cyber security technology products represent common control elements that help secure information technology systems and networks:

• **Access controls** restrict the ability of unknown or unauthorized users to view or use information, hosts or networks. Access control technologies can help protect sensitive data and systems. Access controls include boundary protection, authentication and authorization technologies.

• **System integrity controls** are used to ensure that a system and its data are not illicitly modified or corrupted by a malicious code. Antivirus software and integrity checkers are two types of technologies that help ensure system integrity.

• **Cryptography controls** include encryption of data during their transmission and when they are stored on a system. Encryption is the process of transforming ordinary data

into a code form so that the information is accessible only to those who are authorized to access it. Two applications of cryptography are virtual private networks and digital signatures and certificates.

• **Audit and monitoring controls** help administrators to perform investigations during and after an attack. We describe four types of audit and monitoring technologies: intrusion detection systems, intrusion prevention systems, security event correlation tools and computer forensics.

• **Configuration management and ensurance controls** help administrators view and change the security settings on their hosts and networks, verify the correctness of security settings and maintain the security of operations under duress conditions. We discuss five types of configuration management and ensurance technologies: policy enforcement, network management, continuity of operations, scanners and patch management.

b. Cyber security standards can help provide the basis for the purchase and sale of security products by defining a set of rules, conditions or requirements that must be met by the products. There are three broad categories of standards that govern cyber security technology: (1) protocol security standards; (2) product security criteria, such as Common Criteria protection profiles; (3) operational guidelines. Protocol security standards are interface standards that define points of connection between two devices. Product standards establish qualities or requirements for a product to ensure that it will effectively serve its purpose. Operational guidelines define a process to be followed in order for a security process or system to perform effectively.

Product designers and builders can use protocol and product standards to create and test products to make sure that they meet the criteria set forth by the standards. Buyers can select standard-compliant technology, ensuring that the technology meets the standards.

4. Cyber Security Implementation Issues

Critical infrastructure owners are ultimately responsible for addressing their cyber security needs. For some infrastructure sectors, sector coordinators - individuals or organizations - perform a collective role in helping the entities within their sector to improve cyber security. In addition, state and local organizations have a stake in ensuring that the interests of national security and the public good are addressed, and they have a variety of policy tools that can be used to influence the way the national critical infrastructures are protected, including regulations, grants and partnerships. Many of the challenges are common to all types of critical infrastructures, while some challenges are specific of certain sectors. Concomitantly with the challenges, there are opportunities for action by the government, the critical infrastructure sectors, the individual entities that own critical infrastructures and the technology manufacturers [9].

a. A risk-based framework for infrastructure owners to implement cyber security technologies. On the basis of the results of a risk assessment, infrastructure owners can implement available cyber security technologies to mitigate identified risks. There are several categories of available cyber security technologies that could be used to better secure critical infrastructure systems. However, infrastructure owners also need to bear in mind the limitations of these technologies, as well as the interactions of the technologies with the security processes and the people using the technologies.

✓It is important to think of cyber security in **an overall framework** that includes the following processes: (1) determining the business requirements for security; (2) performing risk assessments; (3) establishing a security policy; (4) implementing a cyber security solution that includes people, processes and technology, in order to mitigate identified security risks; (5) continuously monitoring and managing security.

✓**Risk analysis or risk assessment** is a key component within the overall framework for cyber security. The approach to good security is fundamentally similar, regardless of the assets being protected. A risk management methodology can provide the basic information that is required to make decisions on how to protect an entity's information systems.

✓Because it is impossible to protect computer systems from all attacks, countermeasures identified through the **risk management** process must support three integral concepts of a holistic security program: protection, detection, and reaction. Protection provides countermeasures such as policies, procedures and technical controls to defend against attacks on the assets being protected. Detection monitors for potential breakdowns in the protective measures that could result in security breaches. Reaction, which often requires human involvement, responds to detected breaches, so as to thwart attacks before damage can be done. Because absolute protection from attacks is impossible to achieve, a security program that does not incorporate detection and reaction is incomplete.

✓Organizations have limited resources - people and money - and consequently, they typically **focus on improving cyber security only to the extent that those security needs are necessary** to continue their business operations or are demanded by their customers. According to its own prioritization of these risks, the entity may determine the threat of cyber attacks to be a significant risk that it must mitigate. At this point, the entity can proceed to implement countermeasures to mitigate the risk of cyber attacks, based on its analysis of the cost effectiveness of the countermeasures.

b. Some risks are beyond the control of critical infrastructure sectors. A vulnerability assessment may find that there are dependencies on systems or infrastructures beyond the control of an entity. For example, several sectors are dependent on the electrical grid and the telecommunications infrastructure. Some sectors are dependent on computer systems that are operated by other sectors or by the national government. These

interconnections could lead to the introduction of vulnerabilities and they should be accounted for accordingly. However, because many of these dependencies are beyond the control of the entity, the options for mitigating these potential vulnerabilities may be limited. To account for such a failure, one possible option for the dependent entities is to develop a business continuity plan. As part of a risk management process, a business continuity plan can help an entity to identify its most critical business processes and the actions it can take before and during an outage, so as to mitigate potential risks [10].

c. Critical infrastructure sectors have taken actions to address threats to their sectors. National critical infrastructure protection policy calls for a range of actions intended to improve the nation's ability to detect and respond to serious computer-based and physical attacks and establish a partnership between the government and the private sector. It encourages the private sector to voluntarily take efforts to raise awareness, share information and increase the security posture of their physical and cyber assets. Some infrastructure sectors have taken extensive steps to voluntarily perform these suggested activities. Considering the current efforts of critical infrastructure sectors can help inform legislative decision-making on the need for further government policy-making in order to increase the use of cyber security technologies. The main aspects are the following: coordination of efforts and increasing participation in sector activities; collection and analysis of incident, threat and vulnerability information from sector entities; development of strategies, guidance and standards for improving security; providing methods for the independent validation of software and hardware; raising the awareness about the importance of cyber security; encouraging the performance of vulnerability assessments; sharing critical infrastructure protection-related activity information across sectors; sharing best practices; leveraging existing efforts [11].

In this paper we have described some challenges, threats, risks and vulnerabilities to critical infrastructure as well as the methods to protect and use cyber security technologies that can help secure critical infrastructures from cyber attacks. Some technologies, such as firewalls and biometrics, can help to better protect computers and networks against attacks, while others, such as intrusion detection and continuity of operations tools, help detect and respond to cyber attacks while they are in progress. These technologies can help protect information that is being processed, stored, and transmitted in the networked computer systems that are prevalent in critical infrastructures. Although many cyber security technologies are available, experts feel that these technologies are not being purchased or implemented to their full extent. In addition to the need for a short-term solution to properly implementing current cyber security technologies, there is also a long-term need for cyber security research and for transitioning the research results into commercially available products. Starting from a number of research agendas and the ongoing cyber security research, we have found that a number of research areas need continuous attention. These cyber security research areas include: the composition of secure systems, the security of

network embedded systems, security metrics, the socio-economic impact of security, vulnerability identification and analysis, and wireless security.

NOTES

[1] U.S. General Accounting Office. *Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed*, GAO-10-628 (Washington, D.C.: July 15, 2010).
[2] Computer Emergency Response Team of Estonia, *"Malicious Cyber Attacks Against Estonia Come from Abroad"* (Apr. 29, 2007) and Remarks by Homeland Security Secretary Michael Chertoff to the 2008 RSA Conference (Apr. 8, 2008).
[3] U.S. Office of the Secretary of Defense, *Annual Report to Congress: Military Power of the People's Republic of China 2008* (Washington, D.C.: Oct. 16, 2008).
[4] The New York Times, *Google, Citing Attack, Threatens to Exit China* (Jan. 13, 2010). [5] The New York Times*, Suit Says 2 Chinese Firms Stole Web-Blocking Code* (Jan. 7, 2010).
[6] The New York Times*, China Cyber–Spies Target India, Dalai Lama: Report* (Apr. 6, 2010).
[7] U.S. General Accounting Office. *Technology Assessment: Cyber Security for Critical Infrastructure Protection* (Washington, D.C.: May 28, 2004).
[8] The White House. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C.: May 29, 2009).
[9] U.S. General Accounting Office. *Cyber Security: Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems* (Washington, D.C.: March 16, 2011).
[10] U.S. General Accounting Office. *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*, GAO-08-588 (Washington D.C.: July 31, 2008).
[11] U.S. General Accounting Office. *Critical Infrastructure Protection: Sector-specific Plans' Coverage of Key Cyber Security Elements Varies*, GAO-08-113 (Washington D.C.: Oct. 31, 2007) and *Critical Infrastructure Protection: Current Cyber Sector-Specific Planning Approach Needs Reassessment*, GAO-09-969 (Washington D.C.: Sept. 24, 2009).