The 9th International Scientific Conference
“DEFENSE RESOURCES MANAGEMENT
IN THE 21st CENTURY”
Braşov, November 14th 2014

CRITICAL INFORMATION INFRASTRUCTURE PROTECTION: TOWARDS GLOBAL CYBER SECURITY

Ioana Martin PhD candidate

“Alexandru Ioan Cuza” Police Academy

Abstract

Over the last decades, the Internet and more broadly cyberspace have had a tremendous impact on our society. Our daily life, fundamental rights, social interactions and economies depend on information and communication technology working seamlessly. For cyberspace to remain open and free there should be norms, principles and values that can be applied online. Cyberspace should be protected from incidents, malicious activities and misuse.

Information and communication technology (ICT) has become the backbone of our economic growth and is a critical resource which all economic sectors rely on, keeping alive key sectors such as finance, health, energy and transportation. Although the benefits of this interdependence are great, the fact that many organizations have become entirely reliant on ICT to carry out vital functions is bringing new challenges. Therefore, governments around the world have to be prepared themselves to offer a secure cyberspace for any citizen, national economy and national security.

All these challenges are related to threats and vulnerabilities of the digital network and are incorporated in the concept of cyber security. It’s a priority for governments and super-statal entities to develop a comprehensive security strategy for their networks. To that end, one should develop and fund special institutions to deal with this issue, draft plans for preventing cyber attacks and acting if such an attack occurs, identify the attackers and bring them to justice, and rebuild or repair damaged components of the network.

Keywords: cyber security, cyber attacks, national security, critical information infrastructure, security strategy

1. Introduction

Information revolution and the spread of the Internet are stimulating globalization and allowing companies to conduct business all across the world. Technology is developing quickly, providing a lot of improvements to organizations’ productivity, efficiency and competitiveness. Nowadays, a lot of companies outsource much of their business and are using the Internet to cut down operation costs. Thus, daily, large amounts of data with diffrent degrees of protection are circulating over the Internet.

Considering the benefits brought to social and economic life and the serious consequences of their malfunctioning, modern society has become more and more dependent on the availability, reliability, safety and security of the technological infrastructure.

All these changes also bring new security challenges. Cybercrime is of increasing concern, trafficking in human beings is becoming more and more sophisticated, crossborder organized crime is appearing in new forms and terrorism remains a threat to security[1].

There is a need to build secure and trustworthy systems so that people and businesses can make full use of the potential of the Internet. Ensuring that electronic payments can be made in a secure manner is essential.

New challenges are however emerging, including the use of digital currencies and of online platforms facilitating many forms of serious and organized crimes. The number of cyber attacks is likely to increase in the coming years, despite important measures taken to improve the capabilities to fight cybercrime and strengthen cyber security.

2. Critical Information Infrastructure (CII)

The term "*critical infrastructure*"- CI was first used officially in July 1998, when US president decreed *Executive Order on Critical Infrastructure Protection*[2]. This recognized certain parts of the national infrastructure as critical to the national and economic security of the United States and the well-being of its citizens. On December 17, 2003, the directive was updated through Homeland Security Presidential Directive HSPD-7 for *Critical Infrastructure Identification, Prioritization and Protection*. According to this document the United States has some critical infrastructure that is "*so vital that its incapacitation, exploitation, or destruction, through terrorist attack, could have a debilitating effect on security and economic well-being*"[3]. Later, in 2013, the *Executive Order - Improving Critical Infrastructure Cyber security* stipulated as follows: "*critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters"*[4].

According to the definition accepted by NATO, CIs are those "*Facilities, services and systems that are so vital to the nation that their removal from service or destruction is potentially destabilizing national security, economy, and health of the population and effective functioning of government*".

Today, several infrastructures, such as communication, banking, energy, transportation, and healthcare, are critical, since their disruption, destruction, or loss of integrity can impact a nation's stability. Authorities consider that these facilities must operate at least at a minimum level for public and private sectors to survive.

In the past, many of these systems were physically separated. Starting with the technological boom from 1970s, CIs gradually converged and became dependent on other information structures such as the public telephone network, Internet, satellite and terrestrial wireless networks for a variety of information functions. Technological progress triggered a greater automatization in the operation and control of CI and the creation of special infrastructure. One of the most important CIs, this infrastructure has become the basis for managing and integrating all other CI including new forms of communication, information sharing and trade[5].

In particular, government and military information infrastructures depend on commercial telecommunication providers for everything, from logistics and transport to personnel and other functions. The way these infrastructures are interconnected increase

[1] COM(2014) 154 final

[2] Presidential Directive PDD-63

[3] http://georgewbush-whitehouse.archives.gov/news/releases/2003/12/20031217-5.html

[4] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[5] http://www.comw.org/tct/fulltext/05nickolov.pdf

the effect of a possible malfunctioning that can affect a wide range of different users. Information and information systems both have become an invaluable asset and a lucrative target due to the greater role of information and the availability of electronic means to collect, analyze and modify[6].

3. Threats and Vulnerabilities for CII

ICT evolution made it feasible and convenient to control CIs remotely (e.g., over the Internet). Therefore, industries and governments have been progressively adopting IT systems to consolidate the operation of CIs. As a result, CIs and IT systems have converged and have raised security concerns (and threats). The Internet is a critical asset of modern CIs, because their controlling systems are often distributed over remote, Internet-connected locations. This strong correlation between CIs and their IT comes at the cost of increased complexity and, as a consequence, increased risks of accidental faults. The correct management of non-malicious faults and the management of security risks are strongly correlated, and should always be considered together when planning for the protection of CIs.

Threats and vulnerabilities in cyberspace generally relate to networks, network nodes and vital centers, specifically their physical equipment and systems (computers, providers, network connections and nodes, etc.), and other infrastructure with hosting means (buildings, electricity networks, cable, fiber and other components). Equally, it also covers data warehouses and software, storage systems, storage and distribution of information, databases and more.

But, above all, such threats and vulnerabilities aimed at IT systems (business, product lines, strategic materials supply systems, infrastructure and resources markets, research institutes and communication systems). Threats to cyberspace specific electronic services are by definition global and cannot be contained or controlled within the geographical boundaries. Developing a defense system against those threats should be based on cooperation, both in the detection and analysis, and to implement measures to reduce or cancel the effects of the attacks. Most cyber attacks have exploited known vulnerabilities and common software programming errors. Software publisher vendors have been unable to agree or implement a secure coding standard. Taking into account that most of exploited vulnerabilities are preventable, implementation of a minimum level of software quality is one of the key countermeasures for protecting the CII.

The cyber threat to CI continues to grow and represents one of the most serious national security challenges we must face. The national and economic security of each state in the world depends on the reliable functioning of the national CI in the face of such threats.

The representatives of the insurance company "Aegis London" warned, in a study on global developments in the field of cyber security, about the increasing of cyber threats to the CI, especially in the sectors of energy and water. According to the survey, cyber attacks are increasingly targeted towards operational technologies and critical infrastructure they support, having a significant destructive potential in terms of disruption of services and operation of existing capabilities[7].

[6] http://www.comw.org/tct/fulltext/05nickolov.pdf

[7] http://www.computerweekly.com/news/2240217851/Cyber-threat-moving-to-critical-infrastructure-study-shows

2014 Internet Security Threat Report[8], conducted by "Symantec" (April 15, 2014) revealed that, in 2013, the main countries targeted by cyber attacks were USA, China, India, the Netherlands, Germany, Russia and the UK, Romania being in the 25th position. Although, in the first 10 months of 2013 the small criminal activity was reduced, in the next period, globally there were 8 large-scale attacks, thus registering an increase as compared to 2012, when only one incident of this type was recorded.

The number of security breaches increased by 62% over the previous year, which led to exposure of confidential data of over 552 million people. The document indicates a change in the behavior of cybercriminals: early planning of large-scale attacks; an increased incidence among companies with more than 2,500 employees; high processing techniques.

However, "Symantec" representatives warned (June 30, 2014) that many energy companies in countries like USA, Spain, France, Italy, Germany, Turkey, Poland, Romania, Greece and Serbia are the targets of extensive cyber espionage campaigns. Back in 2011, the group identified as "Dragonfly" is said to have launched a series of attacks on industrial control systems in the power networks and hydrocarbon pipelines capable of generating severe disruption in supply electricity in the countries concerned.

According to a report of the American company "Verizon" (April 22, 2014), government agencies and other public institutions are the most frequently targets of cyber espionage, such security incidents representing in 2013, 75% of all reported globally (63,400). States like USA (54%), South Korea (6%), Japan (4%), Russia (3%) and Ukraine (2%) have reported a high level of cyber espionage. Between "*countries of origin*" of the attacks have been identified China (30%), Romania (28% - their purpose being mainly financial), USA (18%), Bulgaria (7%) and Russia (5%).

The Canadian Security Intelligence Service (CSIS) claims that Canada remains an important target of cyber espionage, given the state advance and expertise in certain areas, particularly the exploitation and extraction of mineral resources and energy. The Canadian Ministry of Natural Resources stated that the most sophisticated attacks are carried out by means of information services which have the necessary financial resources. These attacks are aimed at achieving political, economic, commercial and military advantages. *Communications Security Establishment (CSE)*[9] is one of Canadian government agencies whose work regarding cyber espionage directed to national critical infrastructure is constantly criticized in specialized environments[10].

At national level, in 2013, according to the National Authority for Management and Regulation in Communication (ANCOM), there were 253 cyber incidents with significant impact on electronic communications networks, most of them targeting mobile services. Currently, the authority monitors the implementation of Decision 512 regarding the minimum measures to protect networks and electronic communications services and the reporting system of incidents that affect the security and integrity of networks.

4. **Critical Infrastructure Protection (CIP)**

CIP is nowadays considered the most important objective by all modern countries around the world due to the essential nature of infrastructures' functions and services. National and international securities are more and more dependent of the CIs for society, becoming increasingly vulnerable to sophisticated means of attack.

[8] http://www.symantec.com/content/en/us/enterprise/other_resources/b-str_main_report_v19_21291018.en-us.pdf

[9] coordinated by the Canadian Department of Defense

[10] http://www.torontosun.com/2014/05/20/canada-may-be-on-chinas-cyber-espionage-radar-experts-warn

Traditional security concerns could often be mitigated through government or regulatory actions. Unlike this approach, protecting CIs requires good coordination, collaboration and trust. For organizing effective protective measures public and private organizations, including government agencies, infrastructure owners and operators, and technology vendors must have a good understanding of critical infrastructure risks.

CIP requires a clearly defined partnership between IC owners, operating or management personnel and the authorities, for the development of risk-based standards.

The CIIP action plan has to be built on five pillars: preparedness and prevention, detection and response, mitigation and recovery, international cooperation and criteria for CIs in the field of ICT[11].

The policy has to enhance the security and resilience of CI and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. In order to achieve these goals a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks should be developed. Regarding this aspect there are several initiatives at international, European and national level.

4.1. International

The cyber security framework adopted by NIST, on February 12, 2014, has generated a live debate in the American specialized media on its concrete results in terms of improving the protection and security of computer systems, networks and databases, key components of IC.

One of the issues is about the regulation of voluntary compliance, while the representatives of American industry, including IC operators and owners, are, according to the experts, "*too confident*" about their cyber risk management capabilities.

However, they are still reserved about the allocation of the financial resources for adequate security measures, especially in the absence of higher pressure from federal authorities[12].

Another issue concerns the need to complete the legal framework by adopting ***The National Cybersecurity and Critical Infrastructure Protection Act***, to establish the criteria set for defining the information security in IC sectors[13].

Representatives of the National Association of State Chief Information Officers (NASCIO) demanded[14] concrete actions of the federal authorities for implementing the new cyber security framework. The main requirements are to provide a more flexible mechanism for use of government funds in this area, in line with NIST recommendations.

In the study ***The Critical Infrastructure Protection: Concepts and Continuum*** (published on May 6, 2014), “Microsoft” experts scored three basic principles to ensure CI effective protection:

- Adopting coherent policies and strategies to protect the IC, in accordance with the current dynamics of the risks and threats;
- Implementing an appropriate risk management by improving the capacity of prevention, preparedness, mitigation and response;

[11] COM (2011) 163 final

[12] http://www.reuters.com/article/2014/05/16/us-cyber-summit-infrastructure-idUSBREA4F0OK20140516

[13]http://www.darkreading.com/vulnerabilities---threats/baby-teeth-in-infrastructure-cyber-security-framework/d/d-id/1204437

[14] During a conference in Baltimore (May 6-7, 2014)

- Promoting innovation and investment, in particular by allocating funds for training programs, education and research in the field of IC[15].

According to experts of the Organization for Economic Cooperation and Development (OECD)[16], a new internationally direction in the approach to risk is required. The main argument is the need to promote / conduct consistent actions for prevention, mitigation and emergency response at all levels of government and in collaboration with the private sector[17]. According to the OECD, a society resilient to risks is based on:

- Risk identification and assessment, which helps establish priorities and allocate adequate financial and material resources;
- Supporting investments in prevention, preparedness and response capabilities, including infrastructure protection;
- Promoting good governance in risk management.

For an effective approach to risk, OECD recommendations focused on:

- Implementing national policies in terms of all-hazard concept of risk management;
- Strengthening public-private partnerships, to a more effective response to emergencies;
- Raising awareness of the risk to all policy makers[18].

4.2. European

The directive proposal of the European Parliament and the Council regarding the measures to ensure a common level of network and information security in the EU (NIS)[19] has been an important topic of debate on the conference ***Digital Enterprise Europe 2014*** agenda (London, June 10 – 11, 2014)[20].

Despite the positive vote obtained in the European Parliament (March 13, 2014), the conference participants noted the lack of clarity of the draft legislation regarding:

- The scope (only the companies in the protection IC);
- New security requirements imposed to all stakeholders, including the investment required and the impact of regulatory measures on business;
- The implementation and harmonization of the national legislation for each EU Member State.

Analyzing the results obtained so far by the *European Reference Network for Critical Infrastructure Protection* (ERNCIP), expert Kourt Naoum[21] estimated that it will significantly contribute to improve the protection of CI in Europe. A proposal for the continuation of this project until 2020 is in attention of Directorate-General for Home Affairs of the European Commission. ERNCIP aims to identify innovative, efficient and competitive security solutions and the harmonization of EU test protocols through an integrated network of expertise centers and laboratories[22].

[15] http://blogs.technet.com/b/security/archive/2014/05/06/revised-cybersecurity-papers-on-supply-chain-security-and-critical-infrastructure-protection.aspx

[16] Boosting Resilience Through Innovative Risk Governance report, submitted on May 5, 2014

[17] In the last decade, the total amount of damage caused by natural and man disasters in the OECD and BRIC states was estimated at about 1.5 trillion dollars.

[18] http://www.oecd.org/governance/recommendation-on-governance-of-critical-risks.htm

[19] adopted by the European Commission on February 07, 2013

[20] organized by The European Association for e-Identity and Security (EEMA)

[21] Joint Research Centre, Institute for the Protection and Security of the Citizen (IPSC)

[22] https://erncip-project.jrc.ec.europa.eu/

The activity of the eight thematic groups (TG) within ERNCIP[23] led to a trust environment in the IC protection community. This is a key element in managing security issues by facilitating the exchange of information and best practices among all stakeholders involved in protecting European IC[24].

The European Network and Information Security Agency (ENISA) organized the workshop *CERT's in Europe*[25], with focus on cyber security incidents on industrial control systems. Discussions were focused on ENISA approach on cyber security of industrial control systems, information sharing about threats and possible cyber security incidents from the virtual environment and response capabilities to them.

4.3.National

On April 30, 2014, the Government adopted the draft of ***Romanian cyber security law***, which was posted on the website of the Ministry for Information Society, for public consultation[26].

The law will enable the National Cyber Security System (SNSC) which "*will facilitate proactive and reactive measures of information, monitoring, dissemination, analysis, warning, coordination, decision, restoring and awareness*" of the developments in this domain. The normative act "*defines a unified cyber security terminology and a harmonized action framework for the public institutions*"[27]

5. Conclusions

Worldwide, all the actors from individuals to nation states need to ensure that cyberspace and the systems dependent on it are resilient to attack, in the face of constant growth in the scale and complexity of our networks, and enormous volumes of data and applications. The international community needs to protect digital devices and information infrastructures from malicious entities seeking to steal secrets, to deny their access to critical services, and stop their attempts to exploit others' identities to commit crimes. To achieve this goal CIP has to be a continuous process of managing risk that improve security and resiliency.

The challenges regarding CII are not specific to a certain country and cannot be overcome by any country on its own. ICT and the Internet development trigger a more efficient communication, coordination and cooperation among stakeholders. However, unlike the classical version, threats can now originate from anywhere in the world and, due to global interconnectedness, impact any part of the world. So, cyber security of critical information infrastructures doesn't take account of national boundaries and involves transnational effort in development and harmonization of strategies and cooperation between state institutions and private companies. To that end, the objective of building a coherent and cooperative approach within the EU needs to be embedded into a global coordination strategy reaching out to key partners, such as individual nations or relevant international organizations.

[23] Aviation security, explosives detection, industrial control systems and smart grids, Civil Structures resistance to armed attacks; Biological and chemical hazards in the water supply; Video surveillance; The use of biometric IC protection; Radiological Threats to the IC

[24] The current phase of the project will be completed in the first quarter of 2015

[25] The 9th edition was held in Heraklion, Greece, during May 27-28, 2014

[26] www.mcsi.ro/Transparenta-decizionala/Proiecte-2014

[27] http://www.mediafax.ro/social/guvernul-a-adoptat-proiectul-de-lege-privind-securitatea-cibernetica-12557442

The DAE[28] calls for the "*cooperation of relevant actors [...] to be organized at global level to be effectively able to fight and mitigate security threats*" and sets out the goal to "*work with global stakeholders notably to strengthen global risk management in the digital and in the physical sphere and conduct internationally coordinated targeted actions against computer based crime and security attacks*"[29].

Strategically, the EU needs a more coordinated response. The vision about creating the safest online environment in the world needs to be translated into action. These sustained efforts have to be based on collaboration and information sharing among all key stakeholders—governments, infrastructure owners and operators, and technology vendors.

In Romania, an important step for making SNSC fully operational is the adoption of the cyber security law providing the legal framework that allows the functioning of cyber security mechanisms. Also, other priorities are represented by the development of safety culture and the development of cooperation between the public and private sectors for obtaining real early warning and incident response capabilities.

References

[1] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, on Critical Information Infrastructure Protection '*Achievements and next steps: towards global cyber-security*', Brussels, 31.3.2011, COM (2011) 163 final

[2] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, *An open and secure Europe: making it happen*, Brussels, 11.3.2014, COM (2014) 154 final

[3] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, *A Digital Agenda for Europe*, Brussels, 19.5.2010, COM(2010)245 final

[4] RIZEA Marian, ENĂCHESCU Daniela, NEAMŢU-RIZEA Cristiana, *Infrastructuri critice*, "Carol I" National Defence University Publishing, Bucharest, 2010

[5] ALEXANDRESCU Grigore, VĂDUVA Gheorghe, *Infrastructuri critice. Pericole, amenințări la adresa acestora.* ***Sisteme de protecție*****,** "Carol I" National Defence University Publishing, Bucharest, 2006

[6] SATRC Working Group on Policy and Regulations, *SATRC Report on CRITICAL INFORMATION INFRASTRUCTURE PROTECTION AND CYBER SECURITY*, Adopted by 13th Meeting of the South Asian Telecommunications Regulator's Council 18 – 20 April 2012, Kathmandu, Nepal

[7] Research Center of Cyber Intelligence and Information Security "Sapienza" Università di Roma, *2013 Italian Cyber Security Report. Critical Infrastructure and Other Sensitive Sectors Readiness*, Casa Editrice Università La Sapienza, December 2013

[8] NICKOLOV Eugene, *Critical information infrastructure protection: analysis, evaluation and expectations,* available at http://www.comw.org/tct/fulltext/05nickolov.pdf, accessed in August 5, 2014

[28] Digital Agenda for Europe

[29] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245R%2801%29&from=EN

[9] TABANSKY Lior, *Critical Infrastructure Protection against Cyber Threats, Military and Strategic Affairs*, Volume 3, No. 2, November 2011, available at http://d26e8pvoto2x3r.cloudfront.net/uploadimages/Import/%28FILE%291326273687.pdf, accessed in August 6, 2014

[10] CRONKRITE Mecealus, SZYDLIK John şi PARK Joon, *The Strategies for Critical Cyber Infrastructure (CCI) Protection* by Enhancing Software Assurance, Syracuse University, USA

[11] TUDOSE Mihai, *Identifying the risks towards critical information and communications technology infrastructure*, Scientific Bulletin no. 1 (33) 2012

[12] LEWIS James A., *Cybersecurity and Critical Infrastructure Protection*, Center for Strategic and International Studies, January 2006

[13] ABOUZAKHAR Nasser, *Critical Infrastructure Cybersecurity: A Review of Recent Threats and Violations*, School of Computer Science, College Lane, University of Hertfordshire, Hatfield, UK, 2012

[14] MICROSOFT, *Critical Infrastructure Protection: Concepts and Continuum*, 2014

[15] TENANCE, *Critical Infrastructure Protection: Threats, Attacks and Countermeasures*, March 2014, available at http://www.dis.uniroma1.it/~tenace/download/deliverable/Report_tenace.pdf, accessed in September 1, 2014

[16] SYMANTEC, *Internet Security Threat Report 2014*, volume 19, April 2014, available at http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf, accessed in September 1, 2014

[17] http://www.computerweekly.com/news/2240217851/Cyber-threat-moving-to-critical-infrastructure-study-shows

[18] http://www.reuters.com/article/2014/05/16/us-cyber-summit-infrastructure-idUSBREA4F0OK20140516

[19] http://www.darkreading.com/vulnerabilities---threats/baby-teeth-in-infrastructure-cyber-security-framework/d/d-id/1204437

[20] http://blogs.technet.com/b/security/archive/2014/05/06/revised-cybersecurity-papers-on-supply-chain-security-and-critical-infrastructure-protection.aspx

[21] http://www.oecd.org/governance/recommendation-on-governance-of-critical-risks.htm

[22] https://erncip-project.jrc.ec.europa.eu/

[23] www.mcsi.ro/Transparenta-decizionala/Proiecte-2014

[24] http://www.mediafax.ro/social/guvernul-a-adoptat-proiectul-de-lege-privind-securitatea-cibernetica-12557442

[25] http://georgewbush-whitehouse.archives.gov/news/releases/2003/12/20031217-5.html

[26] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

This work was possible with the financial support of the Sectorial Operational Programme for Human Resources Development 2007-2013, co-financed by the European Social Fund, under the project number **POSDRU/159/1.5/S/138822** with the title ***"Transnational network of integrated management of intelligent doctoral and postdoctoral research in the fields of Military Science, Security and Intelligence, Public order and National Security – Continuous formation programme for elite researchers - "SmartSPODAS"."***