The 10th International Scientific Conference
"DEFENSE RESOURCES MANAGEMENT IN THE 21st CENTURY"
Braşov, November 13th 2015

CRITICAL INFRASTRUCTURES UNDER CYBER THREATS

Virgil-Florin Toșa

Air Force Training School "Aurel Vlaicu" / Boboc / Romania

Abstract:
Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of a modern society and the effective functioning of their government. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence. The cyber-attacks on the SCADA systems of the Iranian nuclear facilities as well as those targeting the telecommunication and power grid infrastructures of Estonia and Georgia show how cyber-attacks against critical infrastructures are becoming increasingly prevalent and disruptive. In the next future, cyber-attacks are expected to increase in scale, to become more accurate and therefore to become real cyber weapons.

Key words: critical infrastructures, cyber security, cyber threats.

1. Introduction

The world has entered a new era called "the information age". The development of new technologies such as mobile telephony, communication satellites, computers, the Internet, has made the world become more interconnected. The development of computers and convergent communication technologies using digital tools for processing, transmission, storage information, changed the entire society activity. Media joined this revolution; we are bombarded almost daily with articles about the new world of cyberspace. Economic publications are awash with business in information technology and communications which incidentally are today one domain - information and communication technology - ICT.

But computer connectivity began in 1969 with the creation of ARPANET - a network of computers which connected four American research institutions: UCLA who was connected in September 1969, Stanford Research Institute in October 1969, the University of California in November 1969 and Utah University in December 1969. The network ARPANET was originally a project of the US DoD, was designed to satisfy business needs and therefore not put security issues. The internet today is known as the enfant terrible of Arpanet network, which over the years has become global network that interconnects people worldwide. Huge amount of money are now transacted through Internet. Strategic Activities are conducted via the Internet as the main means of communication. Also, public services are controlled via the Internet.

Computing power has increased exponentially while reducing the cost per unit, to the point that, nowadays, computers are ubiquitous. Connecting them through the Internet has made communication possible throughout the world with insignificant costs. Access to a computer has allowed a large number of people to obtain various levels of expertise, which was impossible in the past. The positive effects of this technology serving humanity more than any other in the past. The global information infrastructure has become vital

economies in the world so that infrastructure itself became the main target for terrorists worldwide.

Developed countries shall endeavour to create national and global information infrastructure, so-called information highways which originally hoped that they will be paved with "gold and good intentions." The international environment after the Cold War, characterized by information age has proven to have a significant impact on security sector.

Information technology has become one of the integral elements of contemporary society. Whether in your personal life or in professional life, the cyber world has become a dominant factor in everyday life. Most experts agree that the information revolution is the most significant global transformation since the industrial revolution began in mid-century. XVIII. Increasing dependence on information technology contemporary society entailed transforming information systems particularly important targets cyber terrorists which represents a significant threat to military, economic, and ultimately to the national security.

And this information revolution will increase further if not exponentially, even Moore's Law (computer processing power for some costs will be doubles every 18 months).

2. The concept of critical infrastructures

The term *critical infrastructure*, doesn't have an universally recognized definition, or at least a definition that provides a classification suiting the characteristics of each nation. Generally speaking, critical infrastructure is that part of the national infrastructure whose incorrect functioning, even for a short time period, may negatively affect the economy of individual subjects or groups, involving economic losses and/or even expose people and things to a safety and security risk [1].

The EU definition of Critical Infrastructure is "*an asset, system or part thereof located in member states which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a member state as a result of the failure to maintain those functions*" [2]. While a European Critical Infrastructure (ECI) is defined as a "*critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of crosscutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure*". [2]

In Romanian laws, National Critical Infrastructures are defined as "*an asset, system or part thereof located on national territory, which is essential for maintaining vital functions of society, health, safety, security, economic or social well-being of people and whose disruption or destruction would have a significant impact at national level as a result of the failure to maintain those functions*. [3]

United States defines critical infrastructure as "*systems and assets whether physical or virtual, that are 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]

In these three definitions above, there are small differences, but all of them look at identifying potential threats like human error, occasional accidents and attacks that can lead to a malfunction or onset of the crisis of the Critical Infrastructures under observation.

According the European Union Directive 2008/114/EC, there are three criteria for identification of European critical infrastructures:

- potential victims, in terms of number of fatalities or injuries;

- potential economic effects, in terms of financial losses, deterioration of products or services, and environmental effects/damages;
- potential effects on population, in terms of impact on public confidence, physical suffering and disruption of daily life, including the loss of essential services.

With that three criteria, EU defined 11 sectors and 29 sub-sectors (see Table 1).

List of EU Critical infrastructure sectors [5]

Sector		Sub-sector
I	Energy	1 Oil and gas production, refining, treatment, storage and distribution by pipelines 2 Electricity generation and transmission
II	Nuclear industry	3 Production and storage/processing of nuclear substances
III	Information, Communication Technologies, ICT	4 Information system and network protection 5 Instrumentation automation and control systems (SCADA etc.) 6 Internet 7 Provision of fixed telecommunications 8 Provision of mobile telecommunications 9 Radio communication and navigation 10 Satellite communication 11 Broadcasting
IV	Water	12 Provision of drinking water 13 Control of water quality 14 Stemming and control of water quantity
V	Food	15 Provision of food and safeguarding food safety and security
VI	Health	16 Medical and hospital care 17 Medicines, serums, vaccines and pharmaceuticals 18 Bio-laboratories and bio-agents
VII	Financial	19 Payment and securities clearing and settlement infrastructures and systems 20 Regulated markets
VIII	Transport	21 Road transport 22 Rail transport 23 Air transport 24 Inland waterways transport 25 Ocean and short-sea shipping
IX	Chemical industry	26 Production and storage/processing of chemical substances 27 Pipelines of dangerous goods (chemical substances)
X	Space	28 Space
XI	Research facilities	29 Research facilities

Table 1

In the Romanian laws there are some differences: it is included as critical infrastructures the sector for national security (defence, public order and national safety, Integrated border security system, defence industry), the sector of government but the finance sector is completely ignored.

3.Threats

Like any other area of interest to humanity, and critical infrastructures are subject to threats. Among them we'll present only two cases in which critical infrastructure was attacked. One case relates to financial and banking system attacking and the other shows what is believed to be the first weapon used in cyberspace, an attack against a nuclear plant.

3.1 The Carbanak case

Starting late 2013 onwards, a big number (more than 100) of financial institutions suffered an cyber-attack organized and executed by an unknown group of offenders. All these attacks, had the same modus operandi. The cumulative losses of these attack, according to victims and the law enforcement agencies involved in the investigation, was up to 1 billion USD. [6]

What happened ? In Ukraine a bank's ATMs were programmed to spew cash at certain times to people located near them but with no physical interaction according to security cameras. The same scenario happened in Russia later. In order to investigate these attacks, a Russian software company, Kaspersky Lab was involved in a forensic analysis of ATMs dispensing cash. No malware was detected on these ATMs. However, a cyber-malware was found on a computer that was connected to them via VPN – this malware was called Carbanak.

Carbanak is a remote backdoor, created for espionage, data exfiltration and to provide remote control to infected machines. After the access into the victim computer is achieved, attackers perform a manual reconnaissance of the victim's networks. This malware, before proceed to stooling money, made a large reconnaissance including video recordings of the activities of bank employees, particularly system administrators. The videos recorded were sent to the C2 server. With information gained by reconnaissance step, the attackers use different lateral movement tools in order to get access to the critical systems into the victim´s infrastructure. After the victim´s network was compromise, the primary target from inside are money processing services, Automated Teller Machines (ATM) and also, the financial accounts. Sometimes the attackers used the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network in order to transfer money to their accounts.

Please note that the attackers abused the aforementioned services by impersonating legitimate local users who had the permissions to perform the actions later reproduced by the cybercriminals. Of the 100 banking entities was targeted by this malware, at least half have suffered financial losses, with most of the victims located in Russia, USA, Germany, China and Ukraine [6]. This cyber-tool made a huge amount of financial losses.

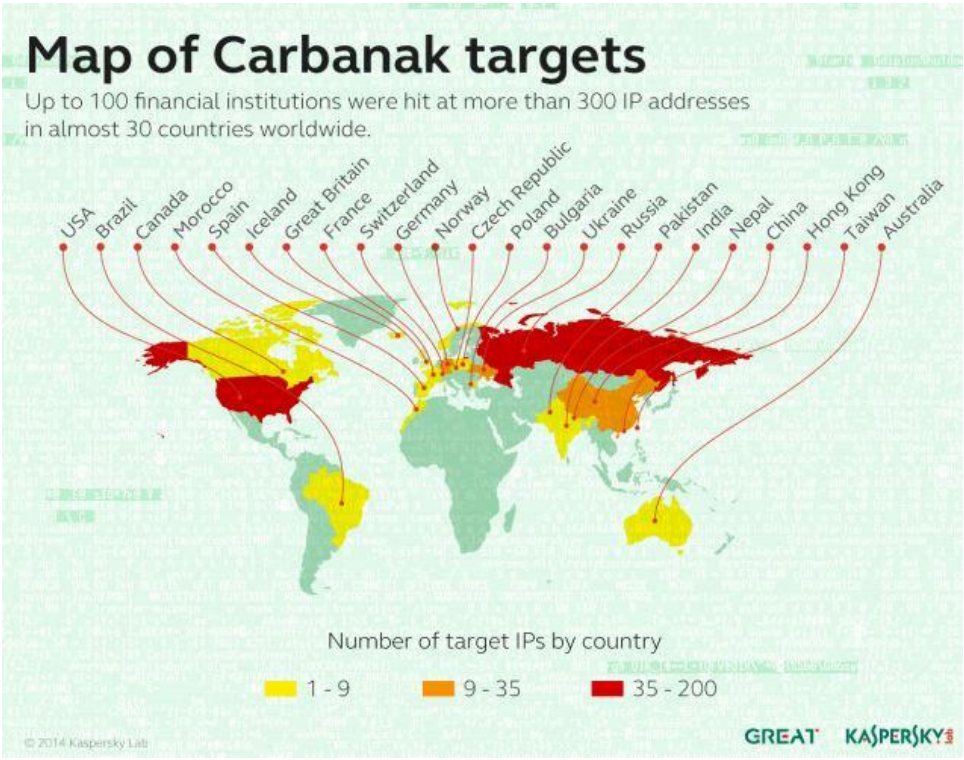


Fig. 1 – Carbanak targets on the world map [6]

This malware prove the importance of applying some strong measures for cyber security even in financial sector.

3.2 Stuxnet – the first cyber weapon

Much of our critical infrastructure is controlled by cyber-physical systems responsible for monitoring and controlling different processes.

The Supervisory Control And Data Acquisition (SCADA) system are industrial control systems responsible for a wide range of industrial processes e.g. manufacturing, power generation, refining, as well as infrastructure e.g. water management, oil & gas pipelines, wind farms, and facilities e.g. airports, space stations, buildings.

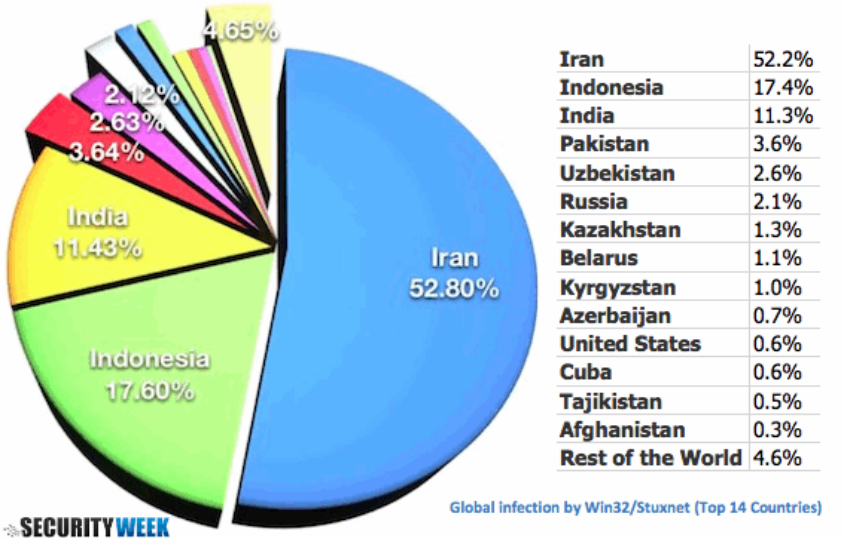
In 2010, the Symantec Corporation, an American technology company headquartered in Mountain View, California, United States, reported about a new and highly sophisticated worm called Stuxnet. This worm became known as the first malware that was used as a cyber-weapon. According to three top management responsible of Symantec Corp, Stuxnet was designed to take control over industrial plant machinery and making them operate outside of their safe or normal performance envelope, causing damage in the process [7].

German expert Ralph Lagner describes this worm: *"Stuxnet is like the arrival of an F-35 fighter jet on a World War I battlefield. The technology is that much superior to anything ever seen before, and to what was assumed possible. An aspect that should be kept in mind is that there is no precedence for this type of attack*" [8].

The Stuxnet generate a deviation from normal comportment of the industrial plant machinery, but this deviation has to be so small for become noticeable only after a long period of time. More than that, great effort was put by the Stuxnet author's in hiding those changes from the operators, even imitating "legitimate" behaviour of instalations. In order to increase the success rate a lot of security holes and vulnerability was used like rootkits.

A geographical analysis (see Figure 2) points out that more than 80% of the infected systems rely mainly in Iran but also in Indonesia and India. Although the main attacks

were detected in mid- 2010, early variants of the Stuxnet piece of code from 2009 have been found. Some analysts believed that the development of this highly sophisticated worm was made by experts from different background and with a massive investment in both time and cost.



Iran	52.2%
Indonesia	17.4%
India	11.3%
Pakistan	3.6%
Uzbekistan	2.6%
Russia	2.1%
Kazakhstan	1.3%
Belarus	1.1%
Kyrgyzstan	1.0%
Azerbaijan	0.7%
United States	0.6%
Cuba	0.6%
Tajikistan	0.5%
Afghanistan	0.3%
Rest of the World	4.6%

Fig. 2. Stuxnet – geographical spread rate [9]

In our days, is known that the target was that industrial systems which had device for controlling the processes (SCADA) furnished by Siemens Company.

The original infection of the Windows computer could be done by simply plugging in a USB stick or from the internal network if an infected machine exists.

Additionally it has installed the first known industrial rootkit which fakes industrial process control sensor signals; hence no alarms or shutdown is done due to abnormal behaviour. This slowly deviating behaviour in combination with the projection of "legitimate" data results in difficulty to assess what is malfunctioning and to pinpoint the faults before it is too late.

According Symantec, this cyber worm device attack modifies the state of the valves used to feed UF6 (uranium hexafluoride gas) into the uranium enrichment centrifuges. Most of them were located in Iran. The worm goal is to closes the valves causing disruption to the flow and possibly destruction of the centrifuges and related systems. Additionally, the worm will take snapshots of the normal running status of the system, and then replay normal operating values during an attack. In this way, the human operators are unaware that the system is not working normally. If the operator tries to change any settings during the course of an attack cycle, the code will prevent modification to the valve status.

4. Conclusion

The problem is that cyber threats successfully demonstrated the feasibility of a very targeted and highly sophisticated cyber-warfare attack. However Stuxnet's design and architecture are not domain-specific and it can be used as a tool for Advanced Persistent Threats (APTs). With some modifications, Stuxnet could be tailored as a platform for attacking other systems e.g. in the nuclear power plants. Its highly sophisticated actions may prevent detection until it is too late.

In the hands of cyber criminals this kind of cyber tools may be a very effective cyber weapon with significant impact over the huge group of people or even countries. The

fear that we may have seen only a successful capability demonstration in 2010, is strengthened by the distribution of modern SCADA and PLC systems over the world, the majority of which rely on USA, EU or Japan. Hence it is imperative to invest on the security as a process by looking holistically the emergent cyber-physical system of systems infrastructures.

The two kind of attacks also show that no sector of business cannot be considered immune to cyber-attacks neither nuclear plants, neither financial sector. It is need for all to constantly be worry about cyber security procedures. So in our opinion even the financial sector is mainly owned by foreign company, it deserve local population and companies and it have to be considered as a critical infrastructures and to be protected as it.

When we discuss about the protection of critical infrastructures, we have to realize we are living in a real, global and interconnected world in which nothing and no one can no longer be considered secure. Every field has become a potential target: citizens, companies, governments. Conventional protection is no longer adequate to block threats, which are becoming more sophisticated and are beyond the majority of control systems.

5.References:

[1] Elgin M. Brunner and Manuel Suter, *International CIIP Handbook 2008/2009. An inventory of 25 national and 7 international critical information infrastructure protection policies*, Center for Security Studies, ETH Zurich, 2008, published on http://www.css.ethz.ch/publications/pdfs/CIIP-HB-08-09.pdf

[2] ***, *European union directive 2008/114/EC*, 2008 published on http://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:32008L0114&from=EN

[3] OUG no. 98 / 3 november 2010 published în Monitorul oficial no. 757 / 12 nov. 2010

[4] ***, *Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) act of 2001*, p.401 published on http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

[5] Commission of the European Communities, *Directive of the council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection* , Brussels, 12.12.2006, published on http://eur-lex.europa.eu/resource.html?uri=cellar:76b1abbf-f028-400b-a9e8-963469ddf736.0003.01/DOC_2&format=DOC

[6] Kaspersky Lab, *Carbanak APT - The Great Bank Robbery*, feb. 2015, on https://securelist.com

[7] Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32.Stuxnet Dossier, Symantec Security Response*, 2011, published on http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-044.pdf

[8] Ralph Langner, *The Big Picture*, 19 November2010, on http://www.langner.com/en/2010/11/19/the-big-picture/

[9] David Harley, *Stuxnet Sux or Stuxnet Success Story ?* , 27sep 2010 on http://www.securityweek.com/