CYBER ATTACKS, MAJOR THREATS AND VULNERABILITIES AGAINST STATES, ORGANIZATIONS AND CITIZENS

Major General (Ret.) Associate Professor Constantin MINCU, Ph.D.*

Abstract: *The author briefly tries to bring to the attention of those interested the complex issue developed globally on cyber risks, threats and vulnerabilities reaching to the "cyber warfare" with direct involvement of some state actors. Some means and vectors of attack are presented, as well as countermeasures to protect the individual users, companies, governmental and military structures. In the end, the article presents the situation in Romania with respect to some measures already taken and others that will be probably taken in the future, particularly in the legislative and administrative sector regarding cyber protection.*

Keywords: cyber-attacks, cyber warfare, brief history, cyber vulnerabilities and threats, NATO, EU.

Many Romanian and foreign authors approached and are still approaching, particularly following year 2005, the complex topic of cyber-attacks made by individual actors and newly by state actors interested, from different reasons, in disorganizing the informational systems of the adversaries, stealing sensitive information, getting important material benefits, or seriously damaging the functioning of some vital public systems such as: medical, financial-banking, civilian and military communications, military command and control, as well as systems of complex weapons, of utilities (electrical power, natural gases, water pipes, transport networks) and vectors as mass-media and cultural institutions.

* Member of the Romanian Academy of Scientists, member of the Honorary Council of Romanian Academy of Scientists, scientific secretary of the Military Sciences Section, phone number 0722.303.015, email: mincu_constantin@yahoo.com.

Lately, a new type of warfare has become present, being increasingly used in front of the computer, whose battlefield is the Internet. The thorough study of all aspects of info-war and cyber-war, as well as their effects on the human civilization is the responsibility of all specialized services and institutions, but also the task of each honest user connected to Internet.

In this paper we cannot exhaust this complex topic but we will try to point out some aspects to show the importance of developing solid systems of protection by actions of the political factor (proper legislation), state institutions with attributions in the field, corporations and trading companies and, last but not least, of each citizen connected to Internet and social media.

1. A brief history of electric and electronic communications and of informatics systems

Although there are many people who know at least sequentially the development of communications and informatics systems, there are few interested in the crucial moments in the rapid development of distance communication. Nowadays, what counts is only the effect of present and future networks to make everything inter-connectable in real-time globally.

Still we may talk about some milestones and historical achievements that made possible nowadays progress:

- 1837 – the electric wired telegraph is created;
- 1854 – the phone is invented;
- 1865 – the construction of terrestrial and subaquatic cables is started;
- 1930 – teletext appears (peoples renounce it in 1990);
- 1872 – important research is performed regarding wireless telegraphy (Loomis - USA);
- 1888 – Hertz discovers the existence of electromagnetic waves;
- 1894 – the first experiments on the broadcast of radio messages are made;
- 1901 – the Romanian Dragomir Hurmuzescu performs research with important results on radio broadcast;
- 1902 – the first radio broadcast of human voice;

- 1917 – the first radio connection airplane – land is made;
- 1917 – 1960: the development of radio communication in the military, governmental and commercial fields;
- 1962 – USA launches the first commercial communication satellite;
- 1964 – „INTELSAT" organization makes the decision to launch communication satellites;
- 1965 – the first communication satellite „INTELSAT-1" is launched. After this event, other commercial and governmental networks also appeared: INMARSAT, EUTELSAT, IRIDIUM, and INTERSPUTNIK.
- Following 1965 the bidirectional **globalization – communications** relation is emphasized;
- **1967 – Time zero of future INTERNET. Pentagon in cooperation with some prestigious US universities starts the achievement of a complex network called ARPANET;**
- 1967 – INTEL Company appears and is specialized in the production of micro-chips (crucial moment in the acceleration of future developments in the field of computers);
- 1970 – the ordinary diskette is created and substantially eases human-machine dialogue;
- 1971 – ARPANET (USA) reaches 15 knots and 23 hosts. It is about a network distributed in the territory to provide the leadership continuity to the governmental and military structures in the situation of a major military conflict;
- 1971 – the first INTEL processor appears known as **„chip"**;
- 1972 – email is introduced on ARPANET;
- 1972 – first local network (LAN) appears called ETHERNET;
- 1973 – **we can already speak about INTERNET**;
- 1981 – „IBM" achieves the first "personal computer" (PC);
- 1982 – in the world there are 5.5 million PCs, and now in 2016 – 4.5 billion;
- 1982 – the useful „MOUSE" appears and eases the interaction to the computer;
- 1985 – MICROSOFT launches „Windows 1.0";

- 1991 – the first INTERNET connections in Romania appear for some universities;
- 1992 – in the world there are 65 million PCs and a million of hosts;
- 1992 – **INTERNET is globalized**;
- 1993 – "**.**ro" domain appears;
- 1996 – citizens and institutions in over 100 countries are connected to Internet;
- 1997 –the EXTRANET concept appears;
- 1998 – the "GRID" concept appears as an extended network with strong connexions;
- 2000 – 100 million computers are connected to the INTERNET;
- 2007 – There can be stated that society is dominated by the power and facilities of internet (politics-elections, business-finances, banking systems, defence, security, mass-media, citizens, etc.).
- 2007 – the emergence and fast spreading of popular networks and sites of socializing and communication (My SPACE, FACEBOOK, YOU TUBE etc.);
- After 2007 - until today (2016) - the networks developed exponentially; thus we can show the following data[1]:

	POPULATION	**Connected to internet**	**Ratio of dissemination**	**% of whole connections in the world**
Worldwide	TOTAL 7.3 billion people	3.367 billion people	46.4%	100%
EU	822 million	604.2 million	73.5%	18%
NORTH AMERICA	358 million	314 million	87.9%	9.3%

[1] www.internetworldstats.com/stats.html

- **Situation in Romania in November 2015**

- Population: 19,861,408;
- Connected to internet: 11,178,477 (56,3% dissemination);
- Connected to FACEBOOK: 8,100,000

- **Ratio of dissemination in some European countries**

- Denmark: 96%;
- France: 84%;
- Germania: 88.4%;
- Hungary: 76%;
- Bulgaria: 56.7%
- Russia: 70.5%;
- Serbia: 66.2%;
- Ukraine: 43.4%.

All the data shown fully prove the globalization of overall informational systems and INTERNET, peculiarly with their use in all the human activity domains.

2. Cyber vulnerabilities and threats

Among the authors who analysed – using a language accessible to the wide public – the complex topic of current information systems and cyber-attacks coming from different sources was the American specialist James F. Dunnigan[2], who along the descriptions of communication and information systems development also presented the unpleasant part of the processes, such as the development of attacks and multiplication of the attackers – individuals, groups or some states.

The specialist stated the cyberwarfare is the fight for supremacy over the Internet and the great share of economy now depending on this computer network. The governmental and military structures are also vulnerable against the individual or state attackers.

Individual or group civilian hackers attack in order to achieve financial and image blows, while the military warriors do it in order to help to win wars, to produce maximum of damage to the economy and armed forces of the adversaries.

[2] James F. Dunnigan, *Noua amenințare mondială – Cyber-Terorismul*, Editura Curtea Veche, București, 2010.

In order to better understand the destructions that cyber attackers can produce we need to recall some elements of the specific vocabulary of this type of actions:

- **Trojans** are programs disguised as legal programs. At the beginning, the Trojan horses were used as pranks and resulted only in some inoffensive jokes. But along the ’80s, they became dangerous, some of them being able to destroy data and programs. Others, once initiated, spread by changing other software with the support of its own routines.
- **Viruses** represent the offspring of the Trojan horses. The virus attaches to a program or authentic document. In the ’90s when the Trojan horses started to rapidly spread on the Internet, they were called informatics viruses.
- **Worms** are viruses attached to other programs. For example, **Logic Bomb**. It is a hidden program in the Computer’s system and is activated only when certain conditions are met.
- **Zombies** (sometimes called *bots* from *robots*) are other types of Trojan horses. Unlike the true Trojan horse programs, zombies are rather controlled (on the internet) by the people inserting them rather than automatically.
- **Vampires** are worms or viruses with the goal to enter deeply in the system, thus rendering the infested computer unable to do anything else.
- **Fishing** refers to hacking instruments for collecting information, going in or out of a computer (usually to the server). Information is afterwards sent to the hacker computer. Fishing is used to collect passwords and IDs of the users.
- **Buffer Overflow Exploitation** is a technique used to send a certain type of data to a web server and is triggered by a software malfunction (common to many Microsoft products), thus letting the hacker fill in a virus or a zombie and thus entering the server despite the defence.
- **There are** also other hacking instruments and sophisticated weapons, in permanent quantitative development and qualitative improvement that can bring trouble to individual users but also to the users of corporations’ and governmental structures.

Let us remember some elements of the cyber threats evolution experienced by NATO, the European Union and the majority of the member

states of these organizations, as well as by other states targeted by the hackers[3]:

- **The attacks executed** with the involvement of a numerous group of computers generating the denial of requested services (distributed denial of service - DDOS), regarded until now as simple forms of "protest blocking", became instrumental in the cyber warfare.
- **In 2007 Red October** virus was launched by a state actor. Most victims were diplomatic, governmental institutions, energy companies, including nuclear energy plants, institutions of scientific research, military contractors and companies within oil and gas industry. The attacks were focused on extracting information from the victims, information offering geostrategic advantages. Important institutions from Romania were also affected by this virus.
- **In 2008,** one of the most serious attacks until now was launched against the American computer systems. By means of a single memory-stick connected to a laptop of the armed forces, in a military base in the Middle East, a spy program spread undetected into classified and unclassified systems. This event accomplished something equivalent with a digital bridgehead by which thousands of data files were transferred to servers under foreign control. Since then the cyber espionage became a constant threat. Similar incidents took place in all NATO state members.
- **In June 2010, „Stuxnet"** malware became public as **„a bomb to penetrate the digital armoured targets"** that attacked the Iranian nuclear program. By this, the early warnings transmitted by the experts starting 2001 became reality, suggesting that the cyber dimension could be used earlier or later to execute some serious attacks with lethal consequences in the real world.
- **During Georgia-Russia conflict** massive attacks were produced against the websites and governmental servers in Georgia offering a more concrete form to the cyber war term.
- **In the summer of 2010** the news was spread that approximately 45,000 **Siemens** systems of industrial control all over the world were infected with a Trojan horse specifically designed able to manipulate technical processes of crucial importance for the nuclear controls in Iran.

[3] http://www.nato.int/dom/review/2011/11-september/Cyber-Threads

Although the assessment of the malfunctions is still unclear, this emphasized the risk of the malware affecting computer systems of main importance for the management of energy supply or of traffic networks. For the first time, there was a proof of the cyber-attacks able to cause real physical malfunctions and to generate the risk of human losses.

- **In February 2013**[4] a strong attack by **Adobe Reader** program was registered. It was not a usual attack; it was an extraordinarily sophisticated attack that could rarely occur. A vulnerability allowed the hackers to copy some files into the system and a second one allowed them to escape from the sandbox. Whoever performed this attack had great abilities as it functions on Adobe Reader systems in Arabic, Hebrew, English and Greek. The conclusion of specialists was that we were dealing with an attack sponsored by a state of the highest level because the attack needed huge resources.
- **After the beginning of the crisis** between Ukraine and Russia (2014) the cyber-attacks against Ukraine were multiplied, as well as the attacks against NATO and EU member states.
- **It is important to mention that if** in 1996 a new virus per week or per month appeared, over 200,000 new viruses now appear daily.
- Nowadays**, Romania** is strongly connected to the Internet and particularly after 2010 is targeted by cyber-attacks over individual users and new targets also became governmental and military institutions and companies.

A balanced assessment of threats clearly proves **two facts:**

- **Until the present**, the most dangerous actors in the cyber field have been nation-states. Despite some offensive capabilities increasingly available to criminal networks able to be used by non-state actors as terrorists in the field of high tech espionage and sabotage in the cyber field, these groups are continuously in need of capabilities, determination and cost-benefit reason of a nation-state.
- **Physical damage** resulting from cyber terrorism has not been produced yet in the real world, but it is clear that attack technology evolves

[4] Costin Raiu, *Laboratoarele Kaspersky*, interview in Adevărul, 19 februarie 2013.

from some annoying problems to a serious threat against the information security and even against the national infrastructures of major importance.

There is no doubt that there are countries massively investing in cyber capabilities to be used for military purposes. At first sight, the digital race of the moment is based on a clear and implacable logic, as cyber warfare offers many advantages: it is asymmetric, attractive by its low costs, and the attacker has – at least in the initial phase – the upper hand.

Moreover, there is no real and practical way to deter cyber war means because even to identify the attacker is extremely difficult and it is almost impossible to defer it to the international law.

Still we can notice many NATO and EU member states develop in accelerated movement defence capabilities in the cyber field starting from the creation of a legal framework to the building of strong technical capabilities and assuring the highest trained specialists in the field.

NATO confronted to the **cyber security challenges** has tried to adapt to this type of threats and vulnerabilities:

- In 2002 it addressed the member states a request regarding the improvement "of their capabilities to defend against cyber-attacks", a part of Prague engagements on capabilities (November 2002).
- **Still, in the years after 2002,** the Alliance focused mainly on the regulation of some passive measures of protection requested by the military part.
- **Events in Estonia** in the spring of 2007 boosted the Alliance to rethink radically its need for a policy in the cyber defence field and to raise its countermeasures to a new level. Therefore, the organization elaborated for the first time a **"NATO Policy on Cyber Defence"** adopted in January 2008, document wherein three core pillars of the policy for the cyberspace were set:

- **Subsidiarity** – the support is provided only on request, otherwise the principle of own responsibility of the sovereign states is applied.

- **Non-duplication**, for example, by avoiding useless duplication to the level of structures or capabilities – internationally, regionally or nationally.

- **Security** – cooperation grounded on mutual trust taking into consideration the sensitivity of the information related to systems which must be made available and the possible vulnerabilities.

• **At the Lisbon Summit** (November 2010), the Alliance successfully set the foundation of a self-managed factual examination of the increasingly complex topic of cyberwarfare.

• **In accordance with the New NATO Strategic Concept,** the revised Alliance's policy on Cyber Defence defines cyber threats as a potential source being the object of collective defence concordantly to Article 5 of NATO. Moreover, the new policy and the "Action Plan" for its implementation offer NATO clear guidelines and an agreed list of priorities on the manner of moving forward the cyber defence of the Alliance.

3. Cyber security – important dimension of national security of Romania

All the world states feel the positive effects of the evolvements in the field of information and communication technologies but as we already have shown they come along with risks, threats and vulnerabilities in the cyber-attack field and even with cyber war. *"These phenomena involve the creation and financing of some institutions to only deal with the cyber security achieving plans to prevent cyber-attacks, to offer the possibility of a rapid response when such events might occur, the ability to discover the persons or organizations responsible for these attacks thus to be brought to justice and nevertheless to gain the ability to timely replace or fix the damaged components of the digital network".*[5]

Cyber security represents a challenge needed to be approached by cooperation between different national actors such as institutions, private companies or nongovernmental organizations, but also on the international level by cooperation between states, regional or global organizations reminding that cyber security is a global concern. Also Romania recognized cyber security as an important dimension of its national security in 2010 when it was included in its **"National Defence Strategy".** This political-military document includes some short and long term objectives related to cyber security because it mentions that our country depends on the good functioning of the multiple networks vital for Romanian citizens' lives and for national economy. In the Strategy it is also acknowledged that Romania

[5] http://www.caleaeuropeana.ro/securitate-securitate-cibernetica-national-romania-cepe/ (Author: Andra Alexandru)

has vulnerabilities in providing national cyberspace security because it has deficiencies regarding the protection and function of digital and critical infrastructure.

Also, the Strategy emphasizes that a higher level of digital infrastructure security is necessary because worldwide the cyber-attacks are increasingly frequent and complex. Thus, Romania regarded certain goals which in time were fulfilled as the establishment of a community of experts in the informatics and digital network security, **CERT-RO** (Romanian National Computer Security Incident Response Team).

CERT-RO is now a functional centre, responsible for the "Prevention, analysis, identification and reaction to cyber incidents" and for developing public policies in this field.

There are also several national institutions involved in activities specific for cyber security, as the Ministry of Communication and Informational Society, Directorate for Investigating Organized Crime and Terrorism (DIICOT), Romanian Intelligence Service, Ministry of Defence, Ministry of Internal Affairs, National Supervisory Authority for Personal Data Processing and also other institutions with limited capabilities. Despite their presence, there is no central institution meant to deal directly and comprehensively with the cyber risks on national level grounded on a cyber security strategy.

We have to mention the fact that the Ministry of Communication and Information Society launched in June 2011 a draft document called **"Romanian Cyber Security Strategy"** which was adopted, in a more complex form, by the Supreme Council of Country's Defence in February 2013.

At the beginning of this year, the draft of **"Law on Romanian Cyber Security"** was launched for public debate. It has not reached yet the parliamentary debate because of its many critics mentioning possible drawbacks generated by impeding on private citizens' life and the confidentiality needed for the business environment. It is still a highly expected and needed document in this phase of the cyber-attacks. Let us hope that by December 31st, 2016 a compromise solution will be reached and the law will be voted and promulgated.

We must show that the cyber security issue is also treated correspondingly in the **"National Defence Strategy Guide for 2015-2019"**

a document approved by Decision of Supreme Council of Country's Defence no. 128 on December 10, 2015.

As it can be noticed, there are plenty of documents, but we consider that more determined practical measures are needed to efficiently respond to the cyber risks, threats and vulnerabilities.

Many Romanian and foreign ITC specialists propose security solutions for individual users, companies and governmental structures, among which we mention:

- A permanently updated security solution to be used;
- All the software programs running on terminals and web servers to be fixed and updated;
- Back-up solutions to be installed;
- Files running in „AppData/Local AppData" directory path to be managed and policies to be provided to stop the users to execute applications or files;
- The access of some persons to some network destinations to be limited;
- Performant protection solutions for email servers to be applied by filtering content;
- Specialized training to be provided to the employees in order for them to be able to identify emails spreading viruses and to avoid accessing them when coming from unknown senders;
- There are also other measures concerning the choice and protection of the password, protection against spyware programs, protection when we use public networks by using Wi-Fi connections (by laptop, phones or tablets).

We mentioned from the beginning that the current and complex topic of cyber-attacks cannot be clarified in a simple article of a journal. The goal is just to show these concerns to the interested people and to discover the best protection solutions.

For a more complete study it is necessary to review dozens of books, studies and articles which is an activity that should pertain to the job description of network administrators and responsible state institutions with direct attributions in ensuring the cyber security of Romania.

BIBLIOGRAPHY

*** *National Defence Strategy* (in Romanian: Strategia Naţională de Apărare), Bucureşti, 2010;

*** *Romanian Cyber Security Strategy* approved by the Supreme Council of Country Defence in February 2013 (in Romanian: Strategia de Securitate Cibernetică a României, aprobată de CSAT, în luna februarie 2013);

*** *Draft of "Law on Romanian Cyber Security"* launched in public debate by MCTI in January 2016 (in Romanian: Proiect de Lege privind Securitatea Cibernetică a României, lansat în dezbatere publică de către MCTI, în luna Ianuarie 2016);

*** *National Defence Strategy Guide for 2015-2019* approved by Decision of the Supreme Council of Country Defence no. 128 on December 10th, 2015 (in Romanian: Ghidul Strategiei Naţionale de Apărare a ţării pentru perioada 2015-2019, aprobat prin Hotărârea CSAT nr. 128, din 10 decembrie 2015);

DUNNIGAN F.James, *Noua ameninţare mondială – Cyber-Terorismul*, Editura Curtea Veche, Bucureşti, 2010;

RAIU Costin, *Laboratoarele Kaspersky*, interview in *Adevărul*, 19 februarie 2013;

www.internetworldstats.com/stats.html;

http://www.nato.int/dom/review/2011/11-september/Cyber-Threads/RO/-index.htm;

http://www.caleaeuropeana.ro/securitate-securitate-cibernetica-national-romania-cepe/;

Other profile websites by using "cyber-attacks" in the search engine.