SOCIOBRAINS
ISSN 2367-5721, JOURNAL HOMEPAGE: WWW.SOCIOBRAINS.COM
INTERNATIONAL SCIENTIFIC REFEREED ONLINE JOURNAL WITH IMPACT FACTOR
ISSUE 32, APRIL 2017

CYBER RESILIENCE – BASIC ASPECTS IN THE SECURITY SECTOR

Abstract: The article analyses the main aspects of cyber security in today's massive use of informationand communicationtechnologies (ICT). The paper reveals and illustrates the relationship between concepts such as cyber attacks, cyber warfare, cyber crime which are basic forthe definition of the term cyber security. An analysis of the factors characterizing cyber resilience has been made as a key element occupying priority positioning the security sector of the country.

Author information:
Ivan Chakarov
LTC, PhD, Chief Assistant Professor,
Communication and Information systems Department
Command Staff Department
Rakovski Nacional DefenseAcademy, Sofia
✉ chakarov_ivan@abv.bg
Bulgaria

Keywords:
Cyber space, cyber-attack, cyber war, internet and information and communications technologies, critical and information infrastructure.

In accordance with the ideas of the universally acknowledged Chinese military strategist Sun Tzu, the author of the famous treatise “Art of War”, which reveals the relationship between war, politics, strategy, tactics, factors and methods, it becomes evident that superiority could be achieved not only through a clearly defined “front line” and “battle" but with the implementation of the full range of methods affecting the communication and information systems for disrupting enemy`s of physical, personal, information and communication security.

The dynamic evolution of information technologies and their application in all spheres of modern life, including the security sector, places new requirements, tasks and challenges to the provision of protection and security of information. This space has been differentiated as a place of war, along with the land, the sea and the air [1]. Today, cyberspace is hosting the "nervous system" of the national critical infrastructure supporting the work of public and private institutions in the field of industry (with military and / or commercial purposes), Information and Communications Technology (ICT) and other sectors. The topics pertaining to cyber-attacks, cyber protection, cyber defense and achievement of cyber sustainability are key areas for debate on every respectable forum on information security. With the advent of the Internet, this "network of networks" has become not only the largest information "bank", but also a realm which concentrates significant potential of critical infrastructure of public and corporate governance, thus increasingly its influence national security.From the analysis of the history and the practice of the executed various cyber-attacks, differentin objectives, scope and intensity, it is apparent that cyberspace from the one hand provides a favorable environment for the transmission of information and numerous opportunities for its use, and from the other hand accommodates the interweaving of diverse interests and poses challenges to the control and regulation of information flows. Thus, the uncertainty generates security risks of the circulating information, regardless of its character (personal or business).From the above - mentioned, it becomes clear that cyberspace is a collection of millions interconnected personal, business and corporate computers, servers, switches, routers, and optical fiber cables, providing and supporting the functionality of the critical infrastructure.

There is a lack of common understanding for cyber-attacks conducted in cyberspace today. The different interpretation of this term by different countries could even lead to escalation of international conflicts. There are definitions of cyber-attacks, such as damage of computers, information, communication networks, or computer-dependent systems [3].The nature of cyber-attacks varies (against a person, against a commercial competitor, criminal ones, terrorist ones), but the technical

means and methods of their implementation are the same and there are three main types of cyber-attacks: physical damage to computers and communication lines, electromagnetic interference, as well as and computers and networks manipulation.

Today, in cyberspace, cyber-attacks are conducted against individual entities or entire communities. Cyber-attacks can pass a certain threshold and become "armed attacks" [1].For that purpose it is necessary to have methods for quantifying the results (effects) from a single cyber-attack.

The next fundamental notion in the field of cyber security is the term “cyber war”.Since the end of the first decade of the XXI century the term cyber war has become a concept of warfare with typical objects and means for battle impact.The closest to my understanding is the definition given by Richard A. Clarke ("Cyber war", 2010)."A cyber war - that is an action of one country penetrating into computers or networks of another country to achieve such goals, which lead to loss or damage."The scope of cyber war coversnot only actions aimed against targets in the security sector (in particular the military systems) but also against those vital to the public infrastructure. The technologies used for attacks in cyberspace are characterized by high speed and broad inclusiveness. Some peculiaritiesof cyber impact may be noted during a cyber war and they include:

- Unidentifiable, with a high degree of anonymity;
- Extreme difficulty to determineits existence and its inception;
- “Malicious software” is used as a major type of weapon:itoperates as multiple programs designed to penetrate other systems and entities before a specific operation.

Cyber-attacks are malicious activities in cyberspace, but not all cyber-attacks can parallel armed attacks.For an example, the failure of Web sites cannot be equal to an act of war, but when the same attack brings about a failure of the power grid of a country and causing material damage and death of people, this contradicts to Art. 2 paragraph 4 of the Charter of the United Nations (UN), which prohibits the use of force against other countries.

In that case, cyber-attacks in the Republic of Estonia in 2007, Syria in 2007 and Georgia in 2008 led to economic and psychological problems in the country, determined by some researchers, as armed attacks. [3]So far no authority has come up with a legal definition for cyber war.

From all the above - mentioned it becomesevident that such events demand qualitative and quantitative measurement of the results of cyber-attacks and cyber wars.Therefore, Professor Michael Schmidt from the European Centre for Development "Marshall", Germany, offers seven criteria for an assessment of operations that use force.

Each of these criteria has a definition and range of meanings:[1,2]

1. Severity - expressed in the number of people killed and thesize of material damage caused by armed attacks, i.e. the size of caused material losses;
2. Immediacy - the time for sequence of actions aimed at getting results. The armed attacks use force on purpose to obtain an immediate effect in terms of seconds or minutes. In some cases (e.g. restriction on trade), the result can be felt for weeks and months;
3. Directness - gives the relation between the operation and theattained result, that is due to the use of force that can be estimated in terms of quantity in various units of measurement;
4. Invasiveness - thedegree to which armed attack crosses the borders of the country. At a lower level the attack is carried out within the initiator country.
5. Measurability - quantification of the results of the operation (military attacks) such as financial dimensions of material damage, results from rupture of diplomatic relations, etc. and a high degree of presumptive legitimacy.
6. Presumptive illegitimacy - determines whether the operation is considered as illegal by the international community, taking into account the absence in the legislation of the possibility for using the armed forces or the presence of a veto for such use.

7. Responsibility - the degree to which the outcome of certain action becomes the property of the country to resist to other participants, provided that the armed compulsion is directed towards its areas which are more sensitive to changes in conditions when external actors use such actions as propaganda and boycott.

In a hypothetical situation, a massive attack against key government websites causes inaccessibility of sites serving thousands of computersfor a day. This corresponds to:

- low to medium degree of burden, because of the lack ofkilled people and direct material damage;
- high degree of immediacy because of the quick result of the attack by "zombing";
- medium to high degree of trend as a result of the breach in the work of devices and software,network monitoring and Internet connections, due to a sharp increase in traffic;
- medium to high degree of assertiveness, due to the deep electronical penetration via the Internet in a foreign territory;
- high degree of measurability determined by the residence time on web servers;
- high degree of alleged illegality - these attacks and the use of force are illegal in valid legislation;
- low to medium level of responsibility - many hackers from a distance could conduct with difficulty an organized propaganda and a boycott;[2]

A question of interest represents the comparison of thedifferent criteria of the above-mentioned cyber-attack. A practical analysis of Schmitt is performed by adding the points for the seven criteria as well as using an average value in more than one criterion.

KEY TERMS USED IN THE FIELD OF CYBERSECURITY:

- Cyberspace - interactive environment of electronic networks and information infrastructure used for creating, destroying, storing, processing, information exchange, management of objects, systems and services;[6]
- Cyberspace (2) - the area in which, IT environment composed of independent networks of information system infrastructures including the Internet, telecommunications networks, computer systems, embedded processors and controllers are used for processing, storage and exchange of information;[6]
- Cyber infrastructure - a combination of people, processes (including managerial) and systems which form cyberspace;
- Cyber services - the different kinds of data exchange in cyberspace for direct or indirect of humans use;
- Critical cyberspace– cyber infrastructure and cyber services that are vital for maintaining public security, economic stability, national security and international stability.

The links betweenthe physical infrastructure, the critical infrastructure and the cyber infrastructure are shown in Figure 1.It is clear that cyber infrastructure underlies the critical infrastructure and the key resources, and therefore, also lies at the heart of the physical infrastructure.The consequences of technological progress lead to the total dependence of these resources on the cyberspace and cyber infrastructure.

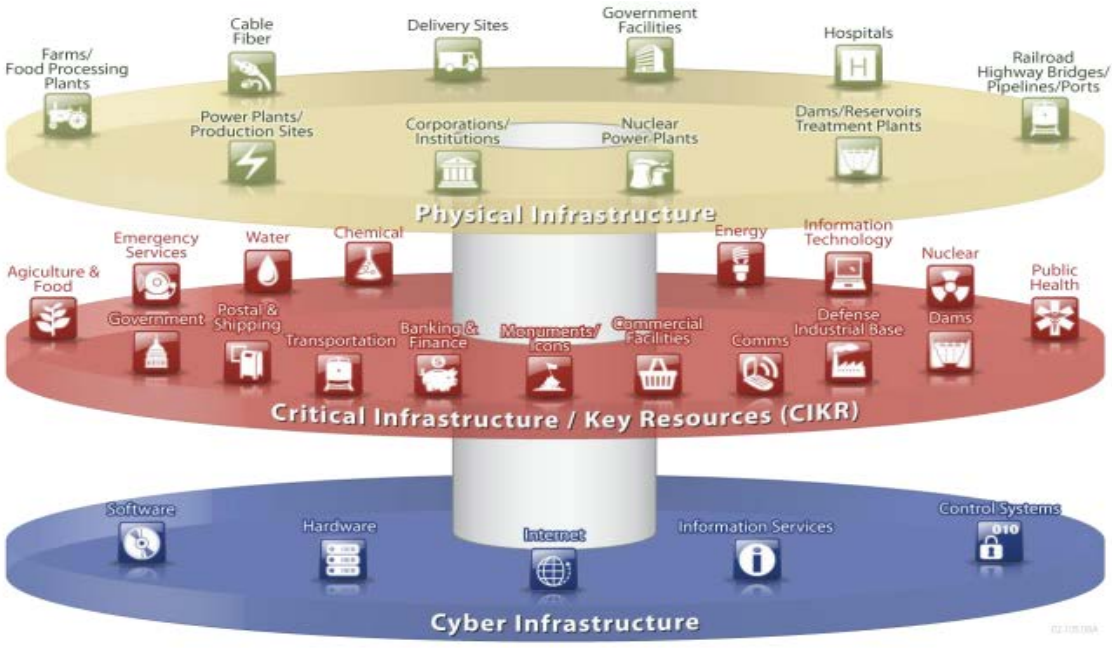

Figure 1: Infrastructure layers

- Critical cyber infrastructure - cyber infrastructure which is essential for providing vital services to maintain public security, economic and international stability, national security, as well as the normal operation and the restoration of critical cyberspace;
- Cybercrime - criminal aims (acts) which are defined in a such way in the national and / or international legislation aimed at and / or using cyberspace;[6]
- Cyber terrorism – the use of cyberspace for terrorist objectives (according to the definitions in the national or international legislation);
- Cyber conflict –a strained situation between states or organized groups in which hostile cyber-attacks provoke retaliation;
- Cyber war - every politically motivated conflict in cyberspace characterized by cyber-attacks on enemy's computer and information systems;[6]
- Cyber security - state defined and measured by the level of confidentiality, integrity, availability, authenticity and fault tolerance of IT resources, systems and services. Cyber security is based on efficient establishment and maintenance of active and preventive measures;[6]
- Cyber-attack - malevolent activity that aims to destroy and provide control over the computing environment / infrastructure, disrupt the integrity of the data or steal controlled information. According to the NATO definition, "…actions taken for violating, rejecting, deteriorating or destroying of information, stored in computer and / or computer network." The types of attacks (acts and / or events) in cyberspace are shown in Figure 2.[6,7]
- Cyber counter-attack - the usage of cyber weapons in order to inflict a deliberate damage on a specific target in response to a cyber-attack;
- Cyber threat - intentional or unintentional acts or events that have the potential or could lead to unpredictable and undesirable adverse effects on cyberspace;
- Cyber capability - the ability for effective protection and / or neutralization of a cyber-attack that can be used as a deterrence factor in cyberspace.

Cyberspace has become the fifth operational domain hostingactivities and operations of any type, including military.

The targets of cyber-attacks and damage that can be caused varyinwidely and are a subject of research, analysis and classification for many organizationswith a view to develop and maintain comprehensive measures for security and protection.Unfortunately, in most cases, cyber-attacks preempt cyber defense, or in other words, cyber-attacks are possible due to technological immaturity of information and communication systems, system and application software, and also because of deficiencies in the system for cyber defense.

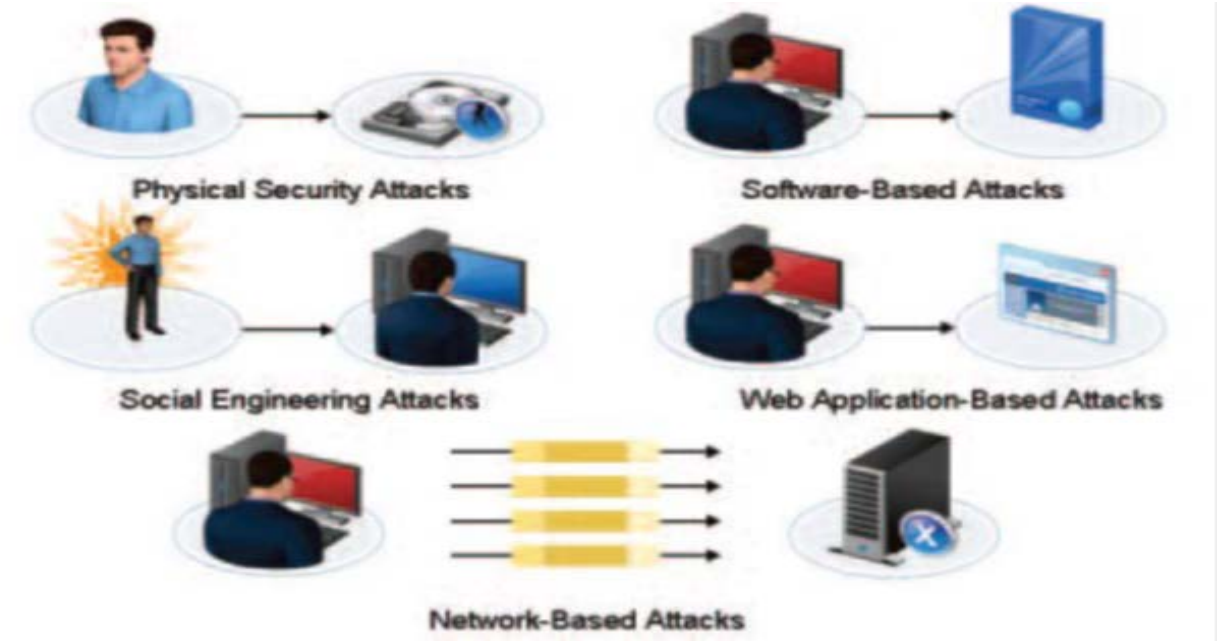

Figure 2: Types of attacks (acts and / or events) in cyberspace

ASPECTS, MEASURES AND FACTORS RELATED TO CYBER SECURITY

After a detailed analysis of the basic concepts outlining cyber sustainability as a key element standing atthe top of the security sector, the various aspects of cyber security should be examined chronologically and they cover the following notions:

1) A set of activities and measures for protection. The activities may include security audits, version management, authentication procedures, access management and others.They may also include assessment of the strengths and weaknesses of hardware and software. The activities may also include detection and reaction to security threats, damage control and recovery of the affected components.Other measures may focus on hardware and software firewalls, physical security as well as personnel training.
2) The state or the quality of the protection against these threats.
3) Scientific research with a view of implementation and improvement of the activities and the *status quo* concerning security.

In these cases, the measures for protection against cyber-attacks include:

- Protection from unauthorized access and theft of confidential and classified information;
- Prevention ofattempts to manipulate existing data and information;
- Limitation of the information lossesresulting from intentional or accidental human errors;
- Forming a culture for safe working environment in the realm of information and communication systems;
- Protection, use of e-mail and contemporary tools such as Facebook, Skype and others.

Cyber security is based on three main types of factors: human, technological and legislative.

The human factor plays an essential role ensuring cyber security ofCIS.This factor depends on the ethical background of the individual and the level of their preparation. The human factor is directly

connected with the process of creation of relevant organizational culture for protection of sensitive and confidential information.The access to the processed and stored information and data must comply with therequirements and the conditions for provision of information and the regulations of the Classified Information Protection Act (CIPA), namely the rule of"need to know".

It is necessary not only to anticipate and to apply measures for backup and storage of data in order to ensure rapid and reliable recovery in case of cyber-attacks or after-crashes, but also it is necessary to work out algorithms and to document recovery procedures.

The technical means are mainly related to hardware and software protection of information and communication systems and can be summarized as follows:

1) Resources for physical provision of computer systems against theft, unauthorized access and improper use;
2) Resources for access control systems (firewalls, passwords, use of biometrics);
3) Resources for Network Intrusion Prevention Systems – NIPS and Network Intrusion Detection Systems – NIDS;
4) Resources for encoding (systems for PKI and private keys);
5) Resources for identification and authentication (digital certificates, markers, electronic signatures);
6) Resources for protection against electromagnetic interference and pulses (EMI / RFI shielding);
7) Resources for network control - usage of appropriate software and hardware (scanners, sniffers, Profilers, Honeypots, Shunts).

It is necessary to coordinate the existing national legislation with those of the member states of NATO and the European Union (EU), in the section pertinent to punitive measures against skilled individuals who create and distribute malware in order to damage and attempt unauthorized access to data and information. The national legislation should addressthe dynamic change in the security conditions thoroughly and promptly.

As a result of the analysis of the trends of the increasing number of cyber-attacks in recent years, it is necessary to define adequate countermeasures for protection.Definitely, there is a tendency towards under-evaluation and even underestimation of the problem. Due to its complexity, these relevant measures should tacklethe technical, technological, physical, legislative and organizational features of the problem.

SUMMARY OF THE MEASURES FOR PROTECTION:

1) Target of potential attacks are not only military structures and missions, but also all government, financial and corporate entities from public and private sectors. All that requires measures on interagency level.
2) The problem transcends national boundaries and clearly demonstrates its international character. All that requires interaction between structures to ensure cyber security of individual countries.
3) In order to counter the rapid spread of cyber-attacks and as a result, limit the amount of damage, it is necessary to establish an effective system for prompt notification of the potential targets of the attack. To this end measures should be taken for the working out of a newsletter about incidents and countermeasures.
4) Furthering the qualification of the personnel in the relevant structures responsible for defense against cyber-attacks and maintenance of a high and uniform (the same for different structures and institutions) level of preparation.
5) Providing a reliable system for backup of critical data and the ability for rapid recovery after a cyber-attack.
6) Effective use of new information technologies for counteraction.

7) Theadoption as a priority task the timely measures for counteraction of manipulative cyber-attacks aiming to create panic and disorientation.
8) In times of economic crisis, fierce competition and aggressive search for markets, one new major target for cybercrime emerges: corporate data bases connected with any possible aspects of the profit-making activity such as the pricing policy, business models, contractual obligations, commercial contacts, scientific research and technological development, etc. Therefore, protection of this type of information must also be subject of consideration for security specialists.[5]

Providing reliable protection against cyber-attacks is related to the implementation of different techniques and technologies such as cryptography, steganography, firewalls, etc. The applications of these techniques and technologies, as well as development of methodology for protection,lie at the basis of the development of the efficient coping strategies for real-time protection against cyber-attacks.

CONCLUSION

From all the above - mentioned, it can be concluded that cyber-attacks have the ability to cause serious damage to the national security and should be treated as an act of war. Today all leading countries in the world invest in cyber security.It is a subject of national security strategies and tailor-made strategies for cyber security. There are already different types of cyber units in the military sphere. Departments and structures responsible for the protection of people and infrastructure entities in a given country should consider cyber security as a major task.

The comprehensive security solution in the cyberspace must include the three vital components of security: prevention, disclosure and reporting of (reaction to) attacks, regardless of their character (internal or external, deliberate or accidental).In spite of the existing research concerning the development of security solutions "end to end," the progress so far has not been significant and universally accepted.Therefore, cyberspace is a global "nervous system" and its protection is a global existential concern.

References:

1. **Beidleman, S., 2009:** Defining and Deterring Cyber War.
2. **Denning, D., 2007:** The Ethics of Cyber Conflict.
3. **Saalbach, K., 2011:** Cyber War. Methods and Practice, Vertion 3.0.
4. **Willke, J., 2010:** Securing the Nation’s Cyber Infrastructure.
5. **Nikolova, D, Bozhilova, M., 2011:** Cyber security’s aspects , 7, CIO.
6. Adopted by Bulgarian Council of Ministers, 2016: National strategy for cyber security “Cyber sustainable Bulgaria 2020”,.
7. **Kalchev, K., 2016:** Kibervoyna – novi aspekti na voennata teorya,7,CIO.