Cytowanie/quotation:
D. Kaźmierczak , *Cyberterrorism, Cybercrime and Cybersecurity,* [w:]red. J. Kuck, Współczesne zagrożenia w zarządzaniu i bezpieczeństwie, UKiP J&D Gębka Gliwice, 2014, ISBN 978-83-64590-00-9; str/p. 439-474

Danuta KAŹMIERCZAK
College of Marketing Management and Foreign Languages in Katowice

CYBERTERRORISM, CYBERCRIME AND CYBERSECURITY

Cyberterroryzm i cyberprzestępstwa a bezpieczeństwo w sieci

Abstract: Contemporary societies are defined as risk societies[1] since the state of permanent risk generated by internal and external factors is its characteristic feature. This results from the level of complexity of contemporary world, its economic and social mechanisms and its new 5th dimension – cyberspace called *IT systems tissue keeping the modern civilization alive*. Cyberspace being a new field of any human activities and so threats, constitutes a crucial element of the state security system. Analyzing acts of terror, their influence and effects as well as defining the actions taken to eliminate them allow to estimate the security level of systems and the real level of cyberterroristic threat also with reference to Polish geopolitical and geostrategic conditions.

Streszczenie: Współczesne społeczeństwa określane są mianem społeczeństw ryzyka. Stan permanentnego zagrożenia, zarówno ze strony czynników zewnętrznych, jak i wewnętrznych przyjmowany jest już obecnie jako coś naturalnego. Bezpośrednią przyczyną jest na pewno stopień skomplikowania współczesnego świata, jego mechanizmów ekonomicznych, jak i społecznych a także jego nowy wymiar - cyberprzestrzeń, *tkanka technologicznej systemów utrzymujących niejako przy życiu współczesną cywilizację*. Stała się ona polem wszelkich działań ludzkich a tym samym newralgicznym elementem systemu bezpieczeństwa państwa ze względu na powstające w niej zagrożenia, w dużej mierze terrorystyczne. Analiza aktów terroru w różnych postaciach, ich siły oddziaływania i skutków a także działań podejmowanych na rzecz

[1]Anthony Giddens http://sociology.about.com/od/Profiles/p/Anthony-Giddens.htm(15.03.2014).

ich eliminacji pozwoli ocenić stopień bezpieczeństwa systemów jak i realny poziom zagrożenia cyberterrorem w odniesieniu również do polskich uwarunkowań geopolitycznych i geostrategicznych.

Is cyberterrorism fear making cowards of us all?

"*Over 100 billion of computers connect us together via incredibly complex arrangement of communication systems, terrestrial and satellite ones….. at the same time state and commercial computing systems are so badly protected today that they can be regarded defenseless. Thus, we are in for the electronic Pearl Harbor*".[2]

Globalization being a product of several factors, mainly scientific and technological development changes the face of the world politically, economically and socially bringing about as many benefits as threats.

Undoubtedly, Internet is the fastest and most efficient means of communication in various forms out of all available technologies (tools).

- enables communication between users on the open source or conditional basis,
- combines all spheres of human activities, e.g.: geographical, economic, social in a seamless way,
- selects information for the given circle of users or communication channels, e.g.: e-mail (one-to-one), newsletter (one-to-many), forum (many-to-many).

Internet is a global network connecting various local networks. OECD defines Internet as the component of many compatible computer networks with the same TCP/IP protocol. Network is the set of computers connected together with the software enabling information transfer to one another.

Table 1

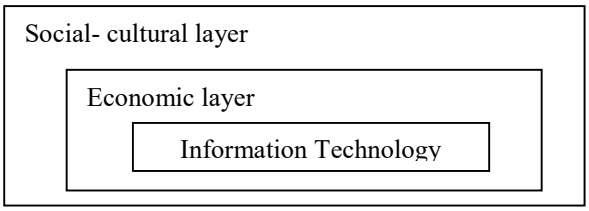
Today and the Near Future.

Today		**2020**
Estimated World Population	7 billion people	~8 billion people
Estimated Internet Population	2.5 billion people (35% of population is online)	~5 billion people (60% of population is online)
Total Number of Devices	12.5 billion internet connected physical objects and devices (~6 devices per person)	50 billion internet connected physical objects and devices (~10 devices per person)
ICT Contribution to the Economy	~4% of GDP on average for G20 nations	10% of worldwide GDP (and perhaps more for developing nations)

[2]A.Toffler, H.Toffler , *Wojna i antywojna*, Wydawnictwo Kurpisz, Poznań 2006, s.172.

Source: National CyberSecurity Framework Manual, NATO.

This spider web of information highways where messages and images run faster and faster creates the cyberspace a new dimension of life for information societies[3] and information constitutes the strategic asset powerful enough to change decision of the enemy at the battlefield or the competitor on the economic market. Certainly, one can recall, at this point, the traditional for social science argument on the nature and direction of forces determining the social development. T. Jordan[4] presents the example of the steam engine. Was it a steam engine that created the industrial society, as K. Marks wished or was it rather rapidly developing capitalistic society which needed new technologies and that need created the steam engine? Relation between technology and society is of complex and multidirectional character. Technology is neither good or bad, or neutral. The society decides about the development of technological solutions. However, the solutions once implemented and accepted determine further social development. Information society can be defined by its layered structure[5]with the core of the information technology surrounded by the layer of economic activities applying these technologies, and this economic layer enveloped by a layer of social, cultural and political processes.



Source: M. Brzozowski, *Organizacja wirtualna,* PWE, Warszawa 2010.

Figure 1. Layered Structure of Information society**.**

The network of these economic, cultural and political connections with fluid state borders alters the world into "global village". Globalization makes the markets and production in given states more and more dependent from one another thus generating

http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf.

[3]*information highway a* term used through the 1990s to refer to digital communication systems and the Internet telecommunications network. It is associated with United States Senator and later Vice-President Al Gore. For the first time the term was coined by A. Targowski in 1970.http://pl.wikipedia. org/wiki/Infostrada (15.03.2014).

Virtual/information society – a group of common interests, hobbies, convictions, needs, life style located in a virtual space , network irrespectively of the real physical position of its members. Chmielarz W., *Systemy biznesu elektronicznego*, Difin, Warszawa 2007, s. 28.

[4]T. Jordan, Hakerstwo, PWN, Warszawa 2011, s. 89.

[5]M. Brzozowski, *Organizacja wirtualna*, PWE, Warszawa 2010, s .12.

the multinational organizations. Above described changes have negative and positive effects for the world. The advantages most often listed are:

- lower prices of products and services,
- higher quality of products and services thanks to technical and organizational development,
- higher demand and smaller deflation risk,
- unlimited access to science, culture, entertainment and leisure achievements,
- less interference of state into the economy,

Disadvantages and threats of globalization:

- social stratification in terms of income,
- increase of unemployment rate in less developed countries,
- limited influence of states on preventing the unemployment,
- threat of global economic crisis.

This rapid technological development and globalization processes interpenetrate and change all spheres of social life, and even one single change in one sphere triggers changes in the remaining ones. Complexity, uncertainty and changeability of the real world create new challenges and economic and social dependencies. Although the basic laws remains unchanged, dynamically changing environment forces formulating and applying new economic and political measures. The most effective methods will be **wars of chaos**, which do not aim any more at massive physical destruction but damage of structures determining the existence of the state, it is critical infrastructure objects[6] which at present are controlled by integrated IT systems. The projection that tomorrow a terrorist can cause more damage with the computer keyboard than with a bomb was confirmed on 11th September 2001 in New York and the subsequent events and analysis provide evidence that the cyberterrorism will be new and more severe form of terror.

So, what does cyberterrorism threaten us with?

Cyberterrorism (called also *soft terrorism*) is the use of Internet based attacks in terrorist activities, including acts of deliberate, large-scale access denial, disruption or destruction of information stored, processed and transferred in computer networks and

[6] Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the state that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. *Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i strategie*, Bellona, Warszawa, s. 99 http://www.dhs.gov/what-critical-infrastructure (15.03.2014).

destruction of these networks. This notion includes also using IT systems to misinform and wage psychological war. The aim of the attack is most often processed information not a system itself. Another definitions are the following:

Dorothy Denning defined cyber-terrorism as "unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives".

James Lewis from the Center for Strategic and International Studies defined cyber terrorismas" The use of computer network tools to shut down critical national infrastructure (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population".

The U.S. National Infrastructure Protection Center defined the term as: "A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to particular political, social or ideological agenda".

The FBI defined cyber terrorism as "The premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub-national groups or clandestine agents".

Mark Pollitt, special agent for the FBI, offers a working definition: "Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub national groups or clandestine agents." He notices that cyberterrorism is the convergence of cybernetics and terrorism. Thus, what are the features of terrorism itself? International terrorism means activities which:

- Involve violent acts or acts dangerous to human life that violate federal or state law,
- Appear to be intended (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping,
- Occur primarily outside the territorial jurisdiction of the U.S., or transcend national boundaries in terms of the means by which they are accomplished, the persons

they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum[7].

Terrorism is a policy or strategy used by many actors of a political stage. … a terroristic attack involves: premeditation, political and psychological aspect, and violence."[8] It is an element of previously planned strategy for the needs of political agenda motivated by religious, ethnic or national reasons. The psychological effect of these acts is to be disproportionately stronger than the extent of material damage, although the violence has also material dimension. There can be state and non-state perpetrators.

Cyberspace' has been defined as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers". There is a widely-held view that it "is not a physical place – it defies measurement in any physical dimension or time space continuum. [9] Yet, cyberspace is more than the internet, including not only hardware, software and information systems, but also people and social interaction within these networks[10]. There can be two different approaches to cyberterrorism[11]:

- when it uses information technology as a tool to organize and carry out attacks,
- when it aims at destroying information technology networks.

Terrorist following hackers may break into state and private computer systems paralyzing military, commercial branches of national economy, state security systems and air traffic control systems. Thus, cyber-terrorism is "the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population." The premise of cyber terrorism is that as nations and critical infrastructure became more

[7]http://www.fbi.gov/about-us/investigate/terrorism/terrorism-definition (15.03.2014).
[8]T. Jordan, *Hakerstwo*, PWN, Warszawa 2011, s. 106.
[9]http://www.ccdcoe.org/publications/2012proceedings/CyCon_2012_Proceedings.pdf (15.03.2014).
C. Czosseck ,R. Ottis, K. Ziolkowski, 4th International Conference on Cyber Conflict, 2012.
[10]Klimburg A., National Cyber Security Framework Manual, NATO, p. 9.
[11]http://www.amw.gdynia.pl/library/File/ZeszytyNaukowe/2005/Sz... (15.03.2014).
Zeszyty naukowe Akademii Marynarki Wojennej. Rok XLVI NR 1 (160) 2005. 173. T. Szubrycht, Cyberterroryzm jako nowa forma zagrożenia.

dependent on computer networks for their operation, new vulnerabilities are created – "a massive electronic Achilles' heel"[12].

From the psychological standpoint the terror is triggered by irrational fear of losing control over computer systems. To justify or make this irrationality credible the example of *robotization of economy* can be quoted here: robots multiplying in factories and institutions, integrated circuits monitoring self-healing of computer networks, intelligent buildings and motorways. Robot-warrior is also a tempting option in the theatre of war, which together with the development of chemical and biological weapon is getting too toxic for a human. Unmanned planes in the Persian Bay considerably lowered losses setting new standard which if to be maintained in the future robots will be a must. Sun-Tsu claimed that to win one hundred times one hundred battles is not topmost achievement… but to defeat the enemy without fight" It is possible to beat the opponent without bloodshed applying modern non-lethal technology. The ideal contractor – terrorist seems to be "robot-vehicle" without moral awareness and fear. Mechanical killer will raise fear among victims and win renown which terrorism needs. From there it's one step to so called "autonomic weapon", which started once makes an independent decisions on its own. It we are to be dependent on them, they have to be super intelligent and learning by experience. The scientists consider also possibility of cooperative groups of robots which communicate with one another. It is imaginable that this group will create collective awareness or even quasi-telepathy.

So the world emerges as one autonomous mega robot with the system of satellite networks and sensors and terrestrial stations. Rational fears evolve from uncertainty, impossibility to project dangers and so organize defense. Terrorists are those who decide when, where and how to conduct the attack. Fear is also enhanced by real plagues with computer viruses, Trojans, insects and logical bombs. At present, experts are afraid of self-controlled virus, which acts as a missile aiming at a specific point. This virus once introduced to the net can lie dormant till started (unconsciously) by a user. There are also programs which can multiply and evolve with the course of time and as a biological organism react to encountered obstacles attaining eventually full

[12] Lewis J., Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic and International Studies, 2002.
http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf (15.03.2014).

autonomy. Pervasive sense of dread is additionally built up by the media announcing series of terrorist attacks which actually are not the cases of terrorism at all.

It is claimed that so far, the Zapatistas attack in Chiapas has been the only classic cyber terroristic attack. Zapatistas opposed to the federal government fighting for Indians' rights, attacked the sites of federal administration typing various slogans, changing them. Connected with hackers – supporters all over the world they paralyzed the whole administration. *It was the first and probably the last example of cyber terrorism i.e. terroristic, politically motivated attack against the government*[13].

Pollit indicates the difference between cyber terrorism and other illegal attacks as computer crime, espionage or cyber warfare.

Liedel also explains clearly that cyber terrorism is an activity of terrorists in a cyber space not attacks of hackers or cybercriminals. Hacker braking into banking system to steal money or entering the administration sites to show off their skills is still a hacker not a terrorist.

If states compete with one another eg. Russia attacks Estonia or China – the USA it is a **cyber warfare** between states not a terrorism which is an **asymmetric conflict** by its nature. Contemporary war is waged by groups of professionally trained soldiers (warriors of knowledge)in cyberspace. In Estonia case Russia was an attacker. At that time the relationship between these countries were spoilt by Estonia attempt at NATO accession. At present NATO has built Cooperative Cyber Defence Centre of Excellence in Tallin.

Whereas Americans in cooperation with Israel used new virus Stuxnet to attack the nuclear power station in Iran and impair nuclear weapon production. This virus penetrated factories and changed the system stealing data through cameras and microphones embedded in computers.

Cyber crime - description[14]:

There are many ways to classify computer crimes. They may be divided according to who commits them and what their motivation might be (e.g., professional criminals looking for financial gain, angry ex-employees looking for revenge, crackers looking for intellectual challenge). Or, by how they are perpetrated (e.g., by physical means such as arson, by software modifications, etc.). Here, computer attacks (they may be

[13]D. Kowalska, *Oswoić strach. Rozmowa o dekadzie terroryzmu z K. Liedelem*., Difin, Warszawa 2011, s. 50.

[14]http://oreilly.com/catalog/crime/chapter/cri_02.html (5.03.2014).

crimes in the legal sense, or only annoyances) are categorized by the types of computer security that ought to prevent them.

***Physical security*:** protection of the physical building, computer, related equipment, and media (e.g., disks and tapes).

***Personnel security*:** protection of the people, computer equipment and data from these people and others in and outside the organization.

***Communications security*:** protection of software and data passing from computer to computer.

***Operations security*:** protection of the procedures used to prevent and detect security breaches, and the development of methods of prevention and detection.

In some cases, the boundaries between these categories may be rather unclear.

The examples of this may be hacking and hactivism.

Hactivism - the practice of gaining unauthorized access to a computer system and carrying out various disruptive actions as means of achieving political or social goals: In this form of hacktivism, the hacker tries to alter or deface a government Website.

Hacktivists people, who for ideological reasons deliberately interfere with online data and services,. They use the same digital tools as the hacker, but does so in order to bring attention to a political or ideological cause. There are no threats to life or health.

Hacktivists are alternatively referred to as ***cyber-activists*.** Another recent neologism on the same theme is ***slacktivist*,** which describes a political activist who may have been active in the past, but now does very little to support a cause, or only does things that require minimal effort. The word ***hacktivist*** is a blend of ***hack*** and ***activist***. The verb *hack* has its origins in the old English ***haccian*,** meaning 'cut into pieces'. The sense relating to gaining unauthorized access to computer data is comparatively recent, dating back to 1983.

Unlike the work of the ***hacker*,** usually associated with criminal activity, especially the illicit transfer of money or sensitive information, hacktivism operates just within the boundaries of legality, exploiting the concept of ***freedom of speech*.** The terms ***hacktivist*** and ***hacktivism*** date back to the mid-1990s, though one of the earliest recorded incidents of the concept in action occurred some years earlier. In October 1989, anti-nuclear protestors wanting to stop a radioactive-fuelled space probe, launched WANK *(*Worms Against Nuclear Killers*),* a program that sabotaged the login screens of NASA computer networks and reportedly cost NASA nearly half a million dollars in wasted time and resources.

Another example from the recent past was the disruption of the websites of a large number of perfume companies, who were targeted by ***green hacktivists*** because they disagreed with the way these firms made and tested their products.

In March 2003 the website of anti-American Arabian TV Al Jazeera stopped working. Instead of the regular image the American flag and inscription "Let freedom sound" appeared. In early 2010, political hacktivists blocked access to a number of Australian government websites in protest at plans to filter content[15].

Breaches of Physical Security.

Dumpster diving, or trashing**,** is searching through materials that have been thrown away. This type of attack isn't illegal in any obvious way or unique to computer facilities. All kinds of sensitive information turns up in the trash, and industrial spies have used this method to get information about their competitors for years.

Wiretapping - telephone and network wiring is often not protected well enough from wiretaps that can pick up the data flowing across the wires. Criminals can use wiretapping methods to eavesdrop on communications. It's easy to tap many types of network cabling. Telephone fraud has always been a problem among crackers, but with the increasing use of cellular phones, phone calling cards, and the ordering of merchandise over the phone using credit cards, this problem has increased dramatically in recent years.

Eavesdropping on Emanations - electronic emanations from computer equipment is mainly a concern for military and intelligence data. Computer equipment, like every other type of any electrical equipment emits electromagnetic impulses. Foreign intelligence services, commercial enterprises, or even teenage crackers may take advantage of these electronic emanations by monitoring, intercepting, and decoding them.

Denial or Degradation of Service.

There are two quite different types of attacks in this category. The first examples of electronic sabotage involve the ***actual destruction*** or disabling of equipment or data. Turning off power or sending messages to system software telling it to stop processing - a classic denial of service.

[15]http://www.macmillandictionary.com/buzzword/entries/hacktivist.html (15.03.2014).

The other type of attack, known as ***flooding*** (or wedging or spamming) is creating new processes that so clog the affected systems that other work cannot be performed. Instead of shutting down service, the attacker puts more and more of a strain on the systems' ability to service requests, so eventually they can't function at all.

Breaches of Personnel Security.

Masquerading - unauthorized password (user's logon ID, password, personal identification number (PIN), or telephone access code) use is the most common type of electronic masquerading, and it's a very effective one. If an outsider steals or figures out a password, there is no easy way for the system cannot tell whether the person who enters the password is the legitimate, authorized user, or an outsider. Unfortunately, passwords are often far too easy to crack.

Social engineering - manipulating others into revealing information that can be used to steal data or subvert systems.

Harassment - sending threatening email messages and slandering people on bulletin board systems and newsgroups. Personally threatening remarks can be simply sent by letter or posted on a wall. But the electronic audience is a much larger one, and such messages, may damage the reputation of the organization as well as individual.

Software piracy is big business of copying and selling off-the-shelf application programs in violation of the copyrights. The problem is an international one, reaching epidemic proportions in some countries. (Software piracy was a major issue in the 1995 Clinton trade agreement with China.)

Breaches of Communications and Data Security

Data Attacks - there are many types of attacks on the confidentiality, integrity, and availability of data. Confidentiality keeps data secret from those not authorized to see it. Integrity keeps data safe from modification by those not authorized to change it. Availability keeps data available for use.

The theft, or unauthorized copying, of confidential data is an obvious attack that falls into this category. Espionage agents steal national defense information. Industrial spies steal their competitors' product information. Crackers steal passwords or other kinds of information on breaking into systems.

Cracking - is the modification of software to remove features considered undesirable, related to protection methods: (copy protection, protection against the manipulation of software), serial number, hardware key, date checks.

Unauthorized Copying of Data.

Piracy is just another example of the unauthorized copying of data.

Traffic analysis - is the analysis of communication. Data that appears valuable to a foreign or industrial spy. Travel itineraries for generals and other dignitaries help terrorists plan attacks against their victims. Accounts payable files tell outsiders what an organization has been purchasing and suggest what its future plans for expansion may be. Even the fact that two people are communicating- regardless to what they are saying to each other--may give away a secret.

Covert Channels - is data leakage. For example, a filename or the contents of a report could be changed slightly to include secret information that is obvious only to someone who is looking for it.

Software Attacks.

A trap door is a quick way into a program; it allows program developers to bypass all of the security built into the program now or in the future.

Session hijacking. Some systems don't disconnect immediately when a session is terminated. Instead, they allow a user to re-access the interrupted program for a short time. A cracker with a good knowledge and skills can take advantage of this fact to reconnect to the terminated session.

Tunneling uses one data transfer method to carry data for another method. Tunneling is an often legitimate way to transfer data over incompatible networks, but it is illegitimate when it is used to carry unauthorized data in legitimate data packets.

Timing attacks are the ways to get unauthorized access to software or data. These include the abuse of race conditions and asynchronous attacks. In race conditions, there is a race between two processes operating on a system; the outcome depends on who wins the race. Asynchronous attacks are another way of taking advantage of dynamic system activity to get access. Computer systems do many things at the same time. The operating system simply places user requests into a queue. A skilled programmer can penetrate the queue and modify the data that is waiting to be processed.

Trojan horse is a method for inserting instructions in a program so that program performs an unauthorized function, e.g.: committing computer-based fraud

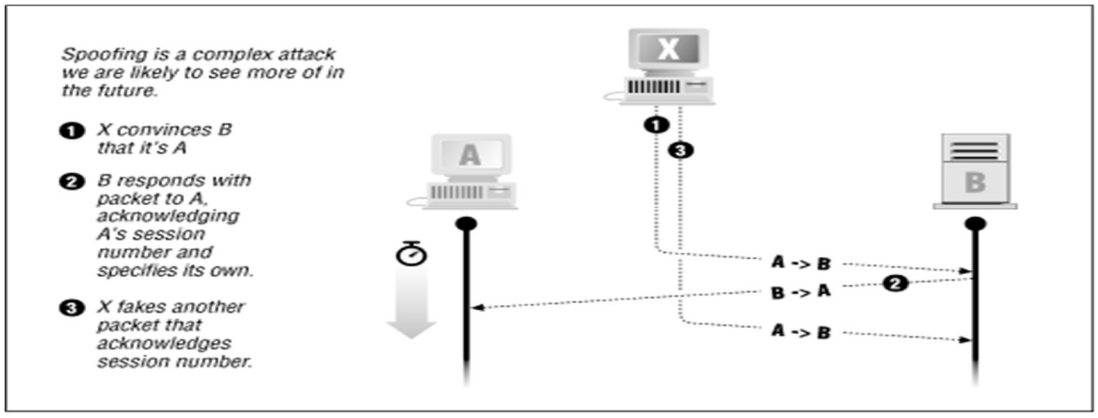
Viruses and Worms. A virus is a program which modifies other programs so they replicate the virus. It can spread if a virus infects a program which is copied to a disk and transferred to another computer, as it could also infect programs on that computer. This is predictable and easy to prevent.

Unlike a virus, a worm exists independently of any other programs. To run, it does not need other programs. A worm simply replicates itself on one computer and tries to infect other computers that may be attached to the same network. A difference between worms and viruses is that a worm operates over a network, but in order to infect a machine, a virus must be physically copied.

A logic bomb tells the computer to execute a set of instructions at a certain date and time or under certain specified conditions.

Breaches of Operations Security.

IP spoofing (Internet Protocol), one of the communications protocols that underlies the Internet) - a method of masquerading. The programs grant access based on IP addresses; the system running the program is authenticated, rather than the individual user. Because the attacker's system looks like an inside system, the user is never asked for a password or any other type of authentication. In fact, the attacker is using this method to penetrate the system from the outside.



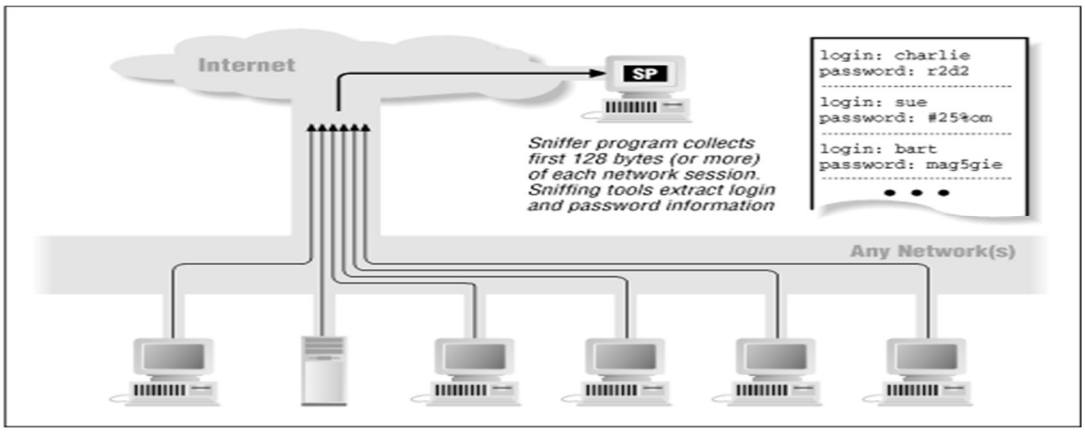
Source: http://oreilly.com/catalog/crime/chapter/cri_02.html(15.03.2014).

Figure 2. IP spoofing, an IP sequence number attack.

Password Sniffing.

Password sniffers are able to monitor all traffic on areas of a network. Crackers installs them on networks used by systems that they especially want to penetrate, e.g. telephone systems and network providers. Password sniffers are programs that simply

collect the first 128 or more bytes of each network connection on the network that's being monitored, e.g.: a user types in a user name and a password are firs typed in information -as required -the sniffer collects that information.



Source: http://oreilly.com/catalog/crime/chapter/cri_02.html(15.03.2014).

Figure 3. Passwordsniffing.

Flooding is a Denial of Service (DoS) attack that is designed to bring a network or service down by flooding it with large amounts of traffic: with connections that cannot be completed.

Phishing - sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into private information for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

For example, 2003 saw the proliferation of a phishing scam in which users received e-mails supposedly from eBay claiming that the user's account was about to be suspended unless he clicked on the provided link and updated the credit card information that the genuine eBay already had. Because it is relatively simple to make a Web site look like a legitimate organizations site by mimicking the HTML code, the scam counted on people being tricked into thinking they were actually being contacted by eBay and were subsequently going to eBay's site to update their account information. By spamming large groups of people, the "phisher" counted on the e-mail being read by a percentage of people who actually had listed credit card numbers with eBay legitimately.

Typosquatting - purchasing a domain name that is a variation on a popular domain name with the expectation that the site will get traffic off of the original sight because of a user's misspelling of the name. For example, registering the domain names webapedia.com or yahooo.com in the hopes that someone making a typo will get to that site unexpectedly.

Cybersquatting is the act of registering a popular Internet address--usually a company name-with the intent of selling it to its rightful owner.

Comparing cybersquatting to online extortion, Senator Spencer Abraham, a Michigan Republican, has introduced to Congress the Anti-Cybersquatting Consumer Protection Act. This bill, if enacted, would make cybersquatting illegal. Violators would be charged a fine of up to $300,000.

The World Intellectual Property Organization (WIPO) has also outlined anti-cybersquatting tactics, which have been endorsed by ICANN (Ironically enough, someone recently registered www.wipo.com in order to sell it back to WIPO for several thousand dollars).

Even though legislation has not been enacted, almost all cybersquatting court-case decisions are against cybersquatters.

Spam**s** end unsolicited bulk messages, especially advertising, most often considered to be electronic junk mail or junk newsgroup postings. Why is it Called Spam?

There is some debate about the source of the term, but the generally accepted version is that it comes from the Monty Python song, **"*Spam spamspamspam, spam spamspamspam, lovely spam, wonderful spam*"**. Like the song, spam is an endless repetition of worthless text. Another idea is that it comes from the computer group lab at the University of Southern California who gave it the name because it has many of the same characteristics as the lunch meat Spam:

- Nobody wants it or ever asks for it.
- No one ever eats it; it is the first item to be pushed to the side when eating the entree.
- Sometimes it is actually tasty, like 1% of junk mail that is really useful to some people.

Spam breaks the netiquette . The organizations fighting with this is Coalition Against Unsolicited Commercial Email (CAUCE) with its branch in Europe from 1999.

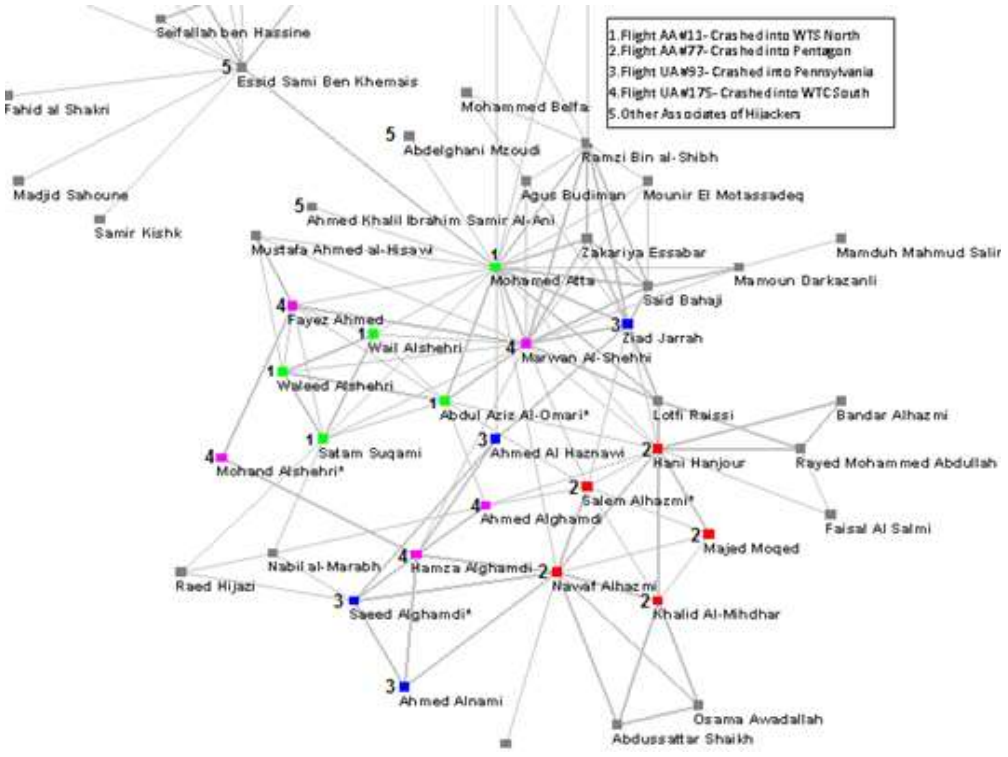
Spying.

Spyware is an application installed before the program and without the user's knowledge. An attempt to uninstall it may result in crashing of the whole system. It is very sophisticated, cryptographic tool impossible to detect. There are anti-spying programs as Ad-Aware or Opt-Out, firewalls.

The example of spying is the Internet analysis of social networks Face book, Twitter, Nasza Klasa, private networks created by organizations and individuals with internet portals. Internet with its transparency gives new ways to analyze this networks and collecting data not only for businessmen but also individuals. The data, information can be used without owners' permission and knowledge.

Business environment analysis can be run for industrial intelligence. The analysis of social networks is useful for criminology to collect information and answer seven "golden questions": who, what, where, how, why, when, with what. The structure of criminal (social) network helps to identify the core, subgroups, behavioral patterns, the elements which cannot be eliminated otherwise the whole network crashes, information and things being transferred in the network.

There are three types of analytical tools. The first generation uses the manual technique and the concept of far-ranging connections in the structure of social network in the Watts – Strogatz Model. After data collecting the matrix is constructed to identify relations between network users. Then the visual graph is created. This technique was used by Kerbsin 2001, creating the net of 19 highjackers of WTC attack on 11 Sept. He analyzed their social relations on the basis of press reports and draw manually the net describing possible patterns of interactions.



*Source: insna.org/PDF/Connections/v24/**2001**_I-3-7.pdf (15.03.2014).*
Figure 4. Trusted prior contacts and meeting ties (shortcuts).

The second generation tools involve the advanced graphic design to visualize the net structure automatically, e.g. Analyst's Notebook, NetMap, Watson (XANALYS Link Explorer). NetMap arranges objects on the fringe of the circle and connects them with lines. The analysis of this connections presents the patterns of interactions between the objects. XANALYS Link Explorer searches through data bases to identify the connections between people and presents the results in a form of diagram.

The third generation tools provides advanced structure analysis to identify members of the core, subgroups and interactional patterns. IBIS is a searching tool for permanent, automatic monitoring of Internet. Maltego system aggregates data in a graphic form. It identifies relations between people or data (phone numbers, e-mail addresses, etc.), communities, organizations, IT structure.

These tools are applied also in business. Polish company IRCenter analyses network societies. Using the crawling technique it chases content on Internet, implement new technologies for social researches: automatic semantic analysis, social network analysis and information diffusion. Yaniva a Altshuler in Ben Gurion University claims that data on social networks are so valuable and big that in the near future it will be the target for cyber terrorists, who will use harmful application and algorithms of advanced network analysis for their own purposes. Julian Assange, creator of WikiLeaks commented on Facebook – this is the most appalling spying tool which has ever been invented.

Criminal acts performed in cybersphere can be classified in terms of effects they bring.

Table 2

Criminal acts performed in cybersphere can be classified in terms of effects:

Character

Illegal acts	Hacking	Spying	Cyberterrorism	Cyberagression

Localization

Territory of the country which is a	International waters International air	Territory of a country used by foreigners	Other country

target in cybersphere	space		

Effects

Small economic causes, IT systems disruption	Small economic causes, disruption of IT systems with victims	Serious economic causes, IT systems disruption	Serious economic causes, disruption of IT systems with victims	Acts which are threat to national security

Source: Zeszyty naukowe Akademii Marynarki Wojennej. Rok XLVI NR 1 (160) 2005. 173. *T. Szubrycht, Cyberterroryzm Jako Nowa Forma Zagrożenia..*

Forms of cyberterrorist attacks: virtual blocking of websites (visiting the page by too big numbers of users at the same time), mail attacks (sending too many mails to one mailbox), hacking, viruses and worms.

Why cyberterrorism?

- Low costs, preparing and performing an attack needs knowledge rather than money. In 1997 National Security Agency organized a simulated attack on Pentagon systems. Hired crackers gained access to number of key systems with only freely available tools on Internet,
- Adjusting means to actions – it is rational choice, maximal effects with minimum of costs, doesn't require suicides,
- Anonymity, it is difficult to check if the attack was prepared by an individual or hired specialist,
- The environment, Internet provide unlimited communication and coordination
- Psychological effect, paralyzing critical infrastructure can cause damage difficult to estimate and remove,
- Dependency of subjects. Security must predict numbers of possible crimes and terrorist can find one weak point, which is a tinderbox (typical asymmetrical conflict),
- Global range, the attack can be performed from any point on the globe. Ex-boss of FBI Jim Settle claims: Give me 10 hackers and during 90 days I will put this country down on knees".

Reasons for cyberterrorist attacks are:

For countries: lack of state security and consistent security policy between owners of infrastructure, legal loops.

For organizations: lack of rules for information protection and security of IT systems, lack of monitoring and error correction, threat analysis, emergency, low level of information protection culture.

For individual: lack of education and using illegal software.

Protection against terrorist attacks can be passive and involve improving and strengthening security systems or can be active aiming at identifying the person responsible, punishing them which is state responsibility. Protection is divided into three stages: prevention, incident management, consequences management.

Prevention:

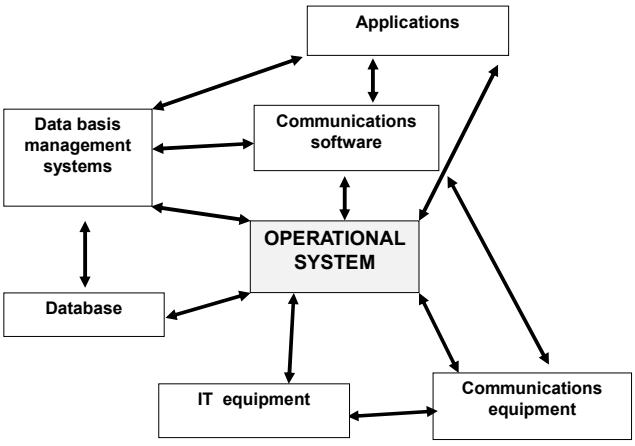
- Implementing protection elements on system designing stage,
- Protection against unwanted person,
- Legal solutions, coordination of international law.

Incident Management: - alarming, immediate identification of the attack

- Strengthening system protection, using the system of codes, firewalls

Consequences Management: - reconstruction of damaged elements, response and revenge

Security of IT Systems.



Source: C.M.Olszak,E. Ziemba, Strategie i modele gospodarki elektronicznej, PWN, Warszawa 2007.
Figure 5. IT System.

A computer information system means a system composed of computer and its related and complementary sets of equipment, tools and facilities (including network) for collecting, processing, storage, transmission, retrieval and other operations of information in accordance with specific application aims and rules. The safety protection of computer information systems should safeguard its safety on all mentioned levels. The most important aspect of data protection are (discussed above):

- confidentiality ensured by coding,
- authenticity (reliability),
- availability (recognized only when the access is blocked because of equipment failure, viruses),
- integrity (information sent and received is the same).

How to protect the information?

There are two basic techniques for encrypting information: symmetric encryption (also called secret key encryption) and asymmetric encryption (also called public key encryption.)

Symmetric encryption is the best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. If both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.

Asymmetric Encryption. The problem with secret keys is exchanging them over the Internet or a large network while preventing them from unwanted disclosure. Anyone who knows the secret key can decrypt the message. One answer is asymmetric encryption, in which there are two related keys -a key pair. A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only you know it.

Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key. Passing public keys over the Internet (the keys are supposed to be public)is not a problem. A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message.

Digital Certificates.

To use asymmetric encryption, there must be a way to discover other public keys. The technique is to use digital certificates (or simply certificates). A certificate is a package of information that identifies a user or a server, and contains information such as the organization name, the organization that issued the certificate, the user's e-mail address and country, and the user's public key. When a server and client require a secure

encrypted communication, they send a query over the network to the other party, which sends back a copy of the certificate. The other party's public key can be extracted from the certificate. A certificate is also be used to identify the holder[16].

The organizations responsible for data security and reliability, authenticity of personal data and identity of individuals and companies using electronic signature and certificates are Certificate Centres. The major ones in Polandare:

The National Certification Centre is the root certification authority for the infrastructure of secure electronic signature in Poland.

At the request of the President of the National Bank of Poland, on the 27 July 2005, the Minister of Economy authorized the National Bank of Poland to perform the following activities[17]:

- generate and issue certificates referred to in Art. 23 of the Act of 18 September 2001 on the electronic signature,
- publish the list of issued certificates,
- publish the data used to verify the issued certificates,
- publish the list of revoked certificates and entrusted the National Bank of Poland with keeping the register of qualified certification service providers.

Polish Security Printing Works (PWPW) [18] offers customers modern, well-secured products and high quality services: banknotes, securities, documents, excise tax bands and postal stamps, as well as plastic cards and electronic services.

Sigillum PCCE[19] is based on the traditions and draws from experience of PWPW in new electronic dimension on the market of securities and electronic services.

Besides the technological solutions for information security the crucial point is to develop the policy of security on what information should be protected, who can have an access to it, and on what conditions, who is responsible for information security management, data processing, what are the emergency procedures and storing copies.

Cyberspace security system:

The European Union Agency for Network and Information Security (ENISA) supported "Cyber Europe 2010", the first pan-European cybersecurity

[16]http://support.microsoft.com/kb/246071 (15.03.2014).
[17]Art. 23, para. 5 and Art. 30, para. 3 of the Act of 18 September 2001 on the electronic signature (Journal of Laws No. 130, item 1450).
[18]http://www.pwpw.pl/produkty_i_uslugi.html (15.03.2014).
[19]http://sigillum.pl/o_nas.html (15.03.2014).

exercise. The objective of ENISA is to improve network and information security in the European Union. ENISA serves as a centre of expertise for both Member States and EU Institutions to seek advice on matters related to network and information security.

Green Paper on a European Programme for Critical Infrastructure Protection. The objective is to protect effectively critical infrastructure, which requires communication, coordination, and cooperation at national and EU level among all interested parties - the owners and operators of infrastructure, regulators, professional bodies and industry associations in cooperation with all levels of government, and the public.

Communication from the Commission of 12 December 2006 on a **European Programme for Critical Infrastructure Protection** [20]The communication sets out the principles, processes and instruments proposed to implement EPCIP. The threats to which the programme aims to respond are not confined to terrorism, but also include criminal activities, natural hazards and other causes of accidents, using an all-hazards approach.

Council Directive[21] of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

USA. The Smart Grid and Cybersecurity - Regulatory Policy and Issues. The "Smart Grid" is the name of the evolving electric power network as new information technology systems are incorporated, which potentially increases the susceptibility of the grid to cyber (i.e., computer-related) attack. The potential for a major disruption or widespread damage to the nation's power system from a large scale cyberattack has increased focus on the cybersecurity of the Smart Grid.

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia[22]aims to be the main source of expertise and enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defense by virtue of education, research and development, lessons learned and consultation.

UN. Resolution adopted by the General Assembly 57/239. Creation of a global culture of cybersecurity, 1998 [23]. It will require that all participants address the

[20] [COM(2006) 786 final – Official Journal C 126 of 7.6.2007]. (15.03.2014).
[21]2008/114/EC of 8 December 2008 (15.03.2014).
[22]https://www.ccdcoe.org/11.html (15.03.2014).
[23]http://search.conduit.com/results.aspx?q=1998+resolution+onz+53%2F70&Suggest=1998+resolution+onz+ 53+70&stype=Results&use

following nine complementary elements: awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, reassessment.

On May 17, 2007, the International Telecommunication Union launched the **Global Cybersecurity Agenda (GCA)** - a global framework for dialogue and international cooperation to coordinate the international response to the growing challenges to cybersecurity.

IMPACT – non-profit organization based in Malaysia in 2008 unites the countries from all over the world to fight cyberterrorism and create global standards.

POLAND. 1997 The Act on Protection of people and property defines the areas, buildings and devices to be protected by professionally armed security formations or responsible for technical security.2005 Regulation on basic requirements for teleinformation security. 2007 The Law on crisis management which fights cyberterrorism as the crime against public order. 2008 CERT.GOV.PL - The Governmental Computer Security Incident Response is a part of the IT Security Department at the Polish Internal Security Agency. Its aim is to ensure and develop the capability of public administration units to protect themselves against cyberthreats[24].

Poland Cybersecurity Strategy 2011-2016[25].

Poland National Security System Strategy 2022[26].

Case study:

- In the 80's western hackers hired by KGB copied confidential data from data bases of USA Department of Defense.
- 1998 Tamil LTTE separatists flooded IT system of Sri Lanka embassy. The technique of flooding is now used by antiglobalists Association pour la Taxation des Transactions pour l'Aide aux Citoyens — ATTAC), and British Globalize Resistance.
- 1999 taking control over UK military satellite.
- 1999 – Matrix operation by USA special troops to paralyze Serbian electronic network. As a revenge Serbian hackers blocked NATO servers.

History=&FollowOn=True&CUI=UN41255265962817430&UM=1&SAT=404&SelfSearch=1&SearchType=SearchWeb&SearchSource=11&ctid=CT3316632&octid=CT3316632 (15.03.2014).

[24]http://www.cert.gov.pl/cee/main-site-about-as/77,dok.html (15.03.2014).

[25]http://www.cybernetyka.org/index.php/portal/msg/40 (15.03.2014).

[26]http://www.bbn.gov.pl/pl/publikacje-i-dokumenty/dokumenty/4901,Strategia-rozwoju-systemu-bezpieczenstwa-narodowego-Rzeczypospolitej-Polskiej-20.html (15.03.2014).

- 1999 Russians cyberspyes stole information about racket control system from USA data bases.
- 2000 Pakistan hackers Club hackers stole numbers of credit cards of about 700 members of American – Israeli Committee on Public Affairs.
- 2000 hired by Hezbollah hackers penetrated IT systems of Israeli Bank and Tel Aviv stock market.
- 2002 Al Kaida members tried to take control over the water system of the biggest USA cities.
- 2003 Arabian hackers tried to disrupt the work of the server of World Jewish Congress.
- 2003-2005 the global spying operation "Titan Rain". Chinese hakers hired by the army searched through the networks of big companies and NASA.
- 2007 Iraqi terrorists used photos of the UK military bases.
- 2007 probably Chinese army attacked the governmental networks of Germany, the UK, France, New Zeeland.
- 2010 attack on Google and 20 other corporations. The epicenter of the attack was China.
- The worm "Here you have" was a reminder of 11th September.
- 2012 Anonymous blocked web pages of Polish PM and ZAiKS to protest against ACTA (Anti-Counterfeiting Trade Agreement).

Projections

Cybercrime is a fact and cyberterrorism still a fiction. A man-bomb" is more effective than taking control over well protected IT systems of critical infrastructure quietly. BinLaden threatened the world with cyberterrorist attacks, claiming that AlKaida is ready to use computers to fight for their cause. However, he used typical terroristic methods.

Why?

The attacks in cyberspace don't produce the expected effect: no dead, no fear, panic. Over the year hundred of attacks on banking systems have been reported but not announced. The same could happen in case of the country. The country attacked in a cyberspace could claim that it was only a system failure.

Terrorists want to attract the attention of the world, which can be achieved by perfect multidimensional manipulation of the media. On their own websites terrorist promote their ideology, communicate on Internet, run courses on how to make a bomb, make films. Terrorist – suicides in Gaza are the true celebrities of Mickey Mouse cartoons.

After analyzing reports experts claim that the probability of cyberattacks is very law and military systems are not threatened. The loses resulted from cyberaggression (25mld) are not estimated on the same level as losses after using weapon of mass destruction (750mld), biological weapon or others (250mld). So far, the cyberattacks haven not been organized by terrorists but other entities, individuals, hackers, countries. Regardless how the attacks in cyberspace are categorized and how threatening they are it is important to prevent the effect of surprise and thoughts about "electronic Pearl harbor"

Technological development and globalization give terrorism different forms of cybercrime, cyberwar or simple cyberteroristic attacks. Undoubtedly, cyberterrorism is a real threat which should not be ignored. Many countries, also Poland introduce the regulations and procedures to secure the cyberspace. The report on security reads that only about 19% of IT systems of Polish public administration is well protected against attacks, 56% is extremely susceptible, 25% - to some degree, which gives total security on the basic level. So, any actions in cyberspace are the challenge for Polish national security, since the economic consequences may be serious and lead to weakening the position on the market and threatening security system.

Bibliography:

Brzozowski M., *Organizacja wirtualna*, PWE, Warszawa 2010.

Jordan T., Hakerstwo, PWN, Warszawa 2011.

Klonowski Z.J., *Systemy informatyczne zarządzania przedsiębiorstwem*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2004.

Kolbusz E., *Inżynieria systemów informatycznych w e-gospodarce*, PWE, Warszawa 2005.

Kowalska D., *Oswoić strach. Rozmowa o dekadzie terroryzmu z K. Liedelem*., Difin, Warszawa 2011.

Olszak C.M., Ziemba E. *Strategie i modele gospodarki elektronicznej*, PWN, Warszawa 2007.

Szpringer W., *Innowacyjne modele e-biznesu*, Difin, Warszawa 2012.

Toffler A, Toffler H., *Wojna i antywojna*, Wydawnictwo Kurpisz, Poznań 2006.

J. Kuck Nowoczesność, Efektywność i bezpieczeństwo współczesnej logistyki, AON, Warszawa 2014.

Red. KuckJ.; *Bezpieczeństwo w procesach globalizacji- dziś i jutro*, WSZMiJO, Katowice 2013.
Red. Wołejszo J., Jakubczak R., *Obronność. Teoria i praktyka*, Bellona, Warszawa 2013.
Red. Podraza A., Potakowski P., Wiak K. *Cyberterroryzm Zagrożeniem XXI wieku*, Diffin, Warszawa 2013.
Red. Szpor G. Wiewiórowski W., *Internet. Prawno-informatyczne problemy sieci, portali*
i e-usług, CH Beck, Warszawa 2012.
Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022 z 9 kwietnia 2013.
Zeszyty naukowe Akademii Marynarki Wojennej. Rok XLVI NR 1 (160) 2005. 173. Szubrycht T., *Cyberterroryzm jako nowa forma zagrożenia*.

Netography:

http://www.crime-research.org/library/Cyber-terrorism.htm.
http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf.
http://www.techterms.com/definition/phishing.
http://www.if.pw.edu.pl/~agatka/moodle/spoleczne.html.
http://www.cs.georgetown.edu/~denning/infosec/pollitt.html.
http://www.prawoautorskie.gov.pl/pages/strona-glowna/obowiazujace-prawo/prawo-autorskie/przepisy-krajowe.php.
http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism/.
http://sociology.about.com/od/Profiles/p/Anthony-Giddens.htm.
http://hal.archives-ouvertes.fr/docs/00/44/74/23/PDF/Boudia-Jas_Risk.pdf.
http://www.ccdcoe.org/publications/books/NationalCyberSecurityFramework Manual.pdf.
http://pl.wikipedia.org/wiki/Infostrada.
http://www.fbi.gov/about-us/investigate/terrorism/terrorism-definition.
http://www.ccdcoe.org/publications/books/NationalCyberSecurityFramework Manual.pdf.
http://www.ccdcoe.org/publications/2012proceedings/CyCon_2012_Proceedings.pdf.
http://www.macmillandictionary.com/buzzword/entries/hacktivist.html.
http://oreilly.com/catalog/crime/chapter/cri_02.html.
http://www.webopedia.com/TERM/S/spam.html.
http://www.amw.gdynia.pl/library/File/ZeszytyNaukowe/2005/Sz...
http://www.dhs.gov/what-critical-infrastructure.
insna.org/PDF/Connections/v24/2001_I-3-7.pdf.