University of Salford
A Greater Manchester University
University of Essex
ESSEX BUSINESS SCHOOL
Centre for Entrepreneurship Research
The General Jonas Zemaitis Military Academy of Lithuania
Ministry of National Defence Republic of Lithuania
World Institute for Engineering and Technology Education
RISEBA
Estonian Business School
Energy Security Center
ENTREPRENEURSHIP AND SUSTAINABILITY CENTER
AVADA

Journal of Security and Sustainability Issues *www.lka.lt/index.php/lt/217049/*
2012, 1(4): 249–260

CYBERTHREATS IN THE SECURITY ENVIRONMENT OF THE 21ST CENTURY: ATTEMPT OF THE CONCEPTUAL ANALYSIS

Robert Białoskórski

The College of Customs and Logistics; 03-301 Warsaw, Jagiellońska 82, Poland
robertbialoskorski@gmail.com

Received 15 March 2012; accepted 15 May 2012

Abstract. The world faces new challenges and threats to international security environment, among which a key role play different types of cyberthreats. This follows, primarily the global links in a cyberspace in terms of critical infrastructure of the state's and intergovernment's objects in the international security environment and the fact that the cyberaggressor's tools are becoming cheaper, and their skills are more and more advanced. There is an urgent need for the analysis of present and future cyberthreats in the security environment, to understand their impact on everone, States, Nations and organizations and develop effective methods of response in this highly complex reality. The article presents the concept of defining of main types of cyberhreats (i.e. information warfare, cyberterrorism, cybercrime and cyberespionage) on the base of the new theoretical approach of modern security environment model.

Keywords: security, war, conflict, information, threats, cyberspace.

Reference to this paper should be made as follows: Białoskórski, R. 2012. Cyberthreats in the security environment of the 21st century: attempt of the conceptual analysis, *Journal of Business Economics and Management* 1(4): 249–260.

JEL Classifications: 031, 032, 033, 033, 038.

1. Introduction

The world faces new challenges and threats to international security environment, among which a key role play different types of cyberthreats. This follows, primarily the global links in a cyberspace in terms of critical infrastructure of the state's and intergovernment's objects in the international security environment and the fact that the cyberaggressor's tools are becoming cheaper, and their skills are more and more advanced. The different links in cyberspace make dependent of all areas of human life on the information and communication technologies, and thus their extraordinary sensitivity and susceptibility on cyberthreats. Particularly, theft and destruction of data and communication systems processing classified information, and control the work of elements of critical infrastructure are severe in consequences. They are a sensitive point in each State and can lead to unpredictable damages in its defence system.

Therefore, there is an urgent need for the analysis of present and future cyberthreats in the security environment, to understand their impact on everone, States, Nations and organizations and develop effective methods of response in this highly complex reality.

2. The concept of security environment

Identification and the role and significance of cyberthreats in the security environment demands primarly specyfying the theoretical idea (concept) of security environment. First of all, it should be noted, that the one common recognized and accepted concept of security environment does not exist, due to its the very complex, multidisciplinary, multidimensional and extremly dynamic nature. Furthermore, the globalisation's processess are creating the security environment increasingly unstable, uncertain and unpredictable (Rotleld 2006, Olchowski, Pietraś 2011). Certainly, this task has to be taken up, during the creating process of the securitology, as a new scientific discipline (i.e. scientific paradigm as the one of necessary conditions).

Taking under consideration, coming from the Abraham Maslow's model of the hierarchy of human's needs fact, that the need for security is the second priority after the physiological one it can be concluded in general point of view, that *security environment is a human and surronding it reality*. It seems to make a sens, that in the globalised world it is difficulty to indicate facts, which affect or do not affect, directly or indirectly, to the security of the individual or society (e.g. philosophy of security, culture of security, education of security).

Stanisław Koziej develops the concept of security environment as "any, external and internal, military and nonmilitary (political, social, cultural, information, etc.) security conditions, the conditions for the realization of the interests of some object in the field of security and the achievement of its established purposes in this regard" (Koziej 2010, p.4). Indicating to the above mentioned security environment conditions, this researcher suggests their parameterizing based on the opportunities, challenges, risks and threats of security. The opportunities are specified as circumstances conductive to the achieving of interests and targets mainly generated by the neutral objects of the security environment and usually having the fast transient nature. The challenges mean dilemmas facing the security objects (international community, states, etc.) in the settlement of security matters. The risks are uncertainties related to the actions, its consequences particularly the adverse effects their actions. Threats of security i.e. the most classical factor of the security environment mean direct or indirect disruptive effects on the object (Koziej 2010).

Figure 1 shows scheme of the concept of security environment defined by Stanisław Koziej.

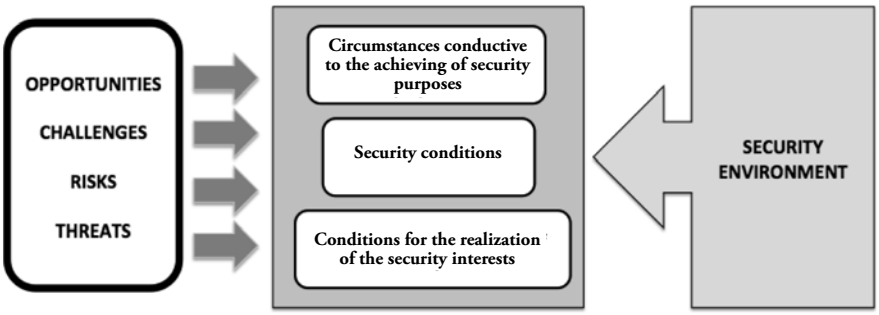

Fig. 1. Scheme of the concept of security environment defined by Stanisław Koziej
Source: Author based on Koziej, 2010.

It should be noted, that both challenges and security threats are presented together in literature very often. They are currently the core of the most security strategies of democratic countries and international organizations, marking the fact of existing so-called "new" challenges and threats now. They are included primarily: uncontrolled proliferation of the weapons of mass destruction and their means of delivery, international terrorism, transnational organised crime, regional and local armed conflicts, problem of the instable States, the growing disparities between rich and poor countries, the increasing demand for the energy sources (Secure Europe 2003).

In fact, all these factors has also existed during the cold war, however they were bound in the shadow of two political-military powers competition. The fall of this world's order has caused their huge eruption and changed their meaning and perception. In this sense cyberthreats belong to the *sensu stricto* new category of security threats, both in terms of their perception, but above all the time, since it emerged so recently.

From another polish researcher Marcin Lasoń point of view, the security challenges mean the new situations, events and circumstances in which appears the necessity to formulate responses and take appropriate actions to protect State before their potencial negative impact.

Security threats in currently international relations are the real actions of the various actors of international scene, adverse and dangerous to their vital interests and the fundamental values. In other words security threats are coincidence of the internal (domestic) or in international relations (external), in which most likely there may be a reduction or loss of the conditions of uniterrupted existence and internal development or breach or loss of State (or group of States) sovereignty and its (their) partner treatment in international relations as a rasult of politically, psychological, economic, military, etc. motivated violence (Lasoń 2010). Such the identification of the security challenges and risks seems correctly, because it clarifies when the se-

curity challenge transforms into security threat. In general sense this goes when there is a likelihood of dangerous situation for environment (Figure 2) (See Białoskórski 2011b, 2011c):

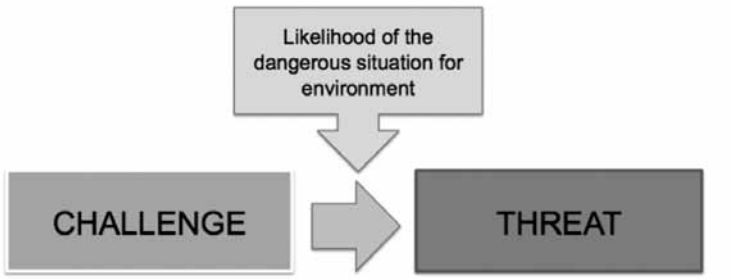

Fig. 2. The general criterium of the transformation process of the security challenge into security threat

Source: Author.

Status of particularly dangerous and destructive interaction in the security environment is an armed conflict. In the narrow sense, the risk of armed conflict may constitute a criterion of transformation the security challenges into security threats. In the case of security threats, risk of armed conflict is the only prerequisite, while security threats are to direct the likelihood of armed conflict. Of course, each security challenge can become a security risk (Figure 3).

However, it has to be noted, the greater distance on the timeline from the critical point of the outbreak of armed conflict at the case of security challenges opposite to the security threats. It means, the grater efficiency of any activities carried out in the framwork of conflict prevention.

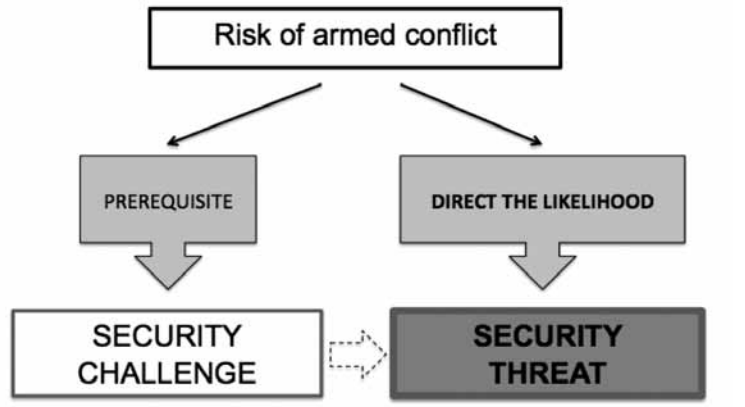

Fig. 3. The criterion of specific transition of security challenge into security threat

Source: Author.

Janusz Ziarko by analyzing the concept of security has recognised three types of components: security objects, security subjects and the reletionship between them (Ziarko 2007). Figure 4 shows a simplified model of security concept by this researcher.

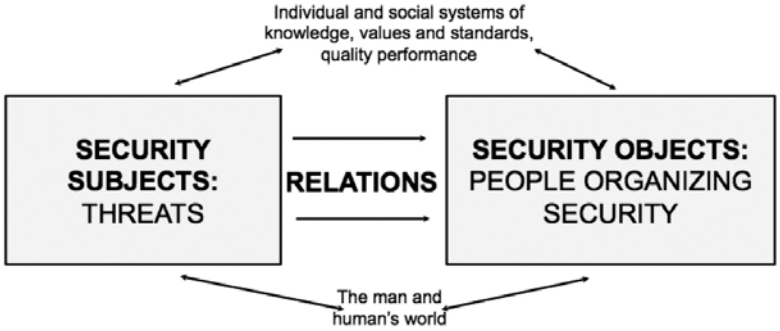

Fig. 4. The simplified model of security concept by Janusz Ziarko

Source: Author based on Ziarko 2007: 12.

Security objects means individuals and various social groups organizing and taking actions in the field of security that is: States, Nations, international organizations (intergovernmental and non-governmental) and the transnational objects (associations, corporations, movements and expressions of solidarity).

The subjects of security means primarily security threats, largerly concerned with attention and determined actions of human activities.

Relationship and the content of security occur both within the security objects and security subjects items, and between them, creating some network of objective links and dependencies.

Similar approach presents Adam Daniel Rotfeld claiming that security is determined by the security threats and the way of their perception and is derived from two factors: responses to existing and emerging threats [implemented by the security objects – author's note] and the way of his perception, which is often more important than facts. This is due to the fact that the response to the threat depends on the way of the perception of reality. In affects, the feeling of the security may be stronger or weaker than the actual status (Rotfeld 2006).

It seems however, that such an approach to the concept of security environment is incomplete, since it takes into account the factor of the "security objects" as the category "people organizing security", so in the positive sense, but it does not take into consideration the negative aspects of this phenemenon, resulting primarily from the two facts:

- first – the same categories "security objects" depends on the "security situation" can generate security challenges and threats, making them *de facto* "objects of danger"
- second – it can be indicated objects that *a priori* generate only the security threats (e.g. international terrorists organizations, international criminal groups) which are not and can not be the security objects, but they are clearly negative actors.

Taking above under consideration, it can be assumed that the security environment consists of two main types of objects:

- environment security objects with their positive and negative impact
- environment security subjects, mainly the security challenges and threats.

Considernig the above, it can be assumed that, in the general point of view, the security environment is the dynamic changing part of the reality consists of a set of security environment components, particularly: security environment objects with their positive and negative impacts and environment security subjects – mainly the challenges and security threats, their characteristics and relations between them, directly or indirectly impact on human security as well in individual (personal) and social sense (Figure 5).

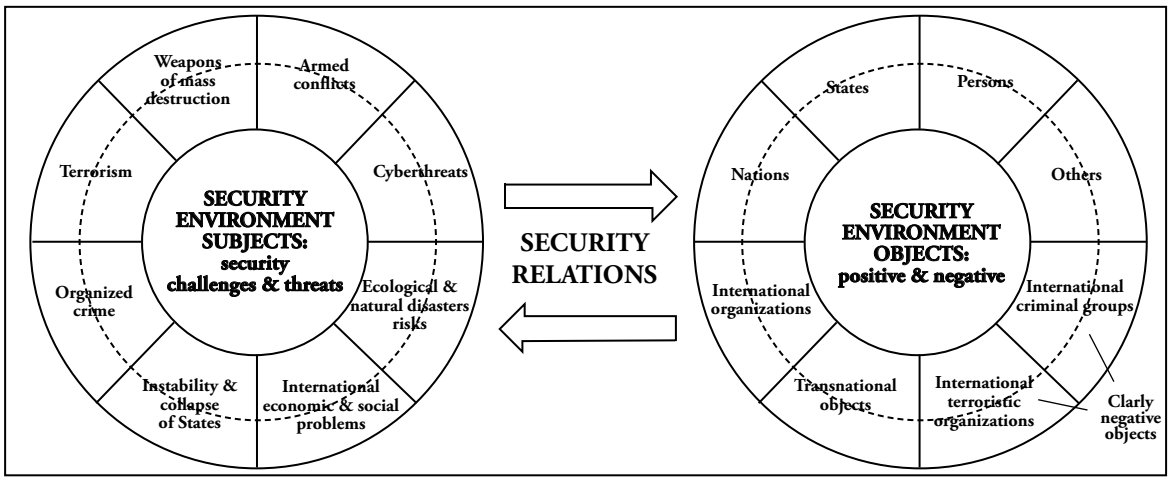

Fig. 5. The simplified model of security environment concept
Source: Author.

The main security evnironment objects include:
a) entities with positive and nagative influence:

- Persons – individual or small unorganized small groups
- States – the principle objects; relations between States still constitute a major axis of international relations, despite the increasing role of non-state actors
- Nations – state the backbone of modern States and

constitute the deepest their identity characteristics

- International organizations (IO's) – institutionalised forms of cooperation between the various actors of international relations; intergovernmental (interstates) organizations (IGO's) and international non-governmental organizations (INGO's)
- transnational objects (TNO's) – include the transfer of some material and spiritual goods over national regulations and outside State control; associations, multinational companies (transnational corporations), movements and expressions of solidarity, Private Military Companies (PMC).

b) entities *stricte* negative interacted:

- international terrorist organizations
- international (transnational) criminal gropus.

To the major contemprary challenges and security threats belong (Białoskórski 2010):

- armed conflicts – particularly internal and local conflicts
- weapons of mass destruction and means of delivery (notably ballistic missiles); in particular nuclear weapon and the pursuit of its possession by the international terrorist organizations
- international terrorism
- transnational organized crime
- instability and collapse of States
- international economic and social problems
- ecological and natural disasters risks
- cyberthreats.

The sources of challenges and security threats are varied and evolving, following with the development of international relations, the changing interests of States, playing a key role on the international scene, the meaning of international organizations and the military technology transitions, as well as the relationships between the major actors (Żukrowska, Grącik 2005).

Cyberthreats - pointed above as the last on the list – will state in the future, the main category of security threats.

Actually, NATO's strategic concept 2020 recognises cyberattacs as one of the main security threats and the legal system of the United States permits the treatment of cyberattacs on critical infrastructure elements of the State from foreign countries as an act of war, which opens the ability to react with the use of armed forces (Department 2011; NATO 2010).

3. Cyberspace as a sphere of cyberthreats

As it was already mentioned, among the many modern challenges and security threats, cyberthreats should be undoubtedly deserved as "new" *sensu stricto*. They had been generated in cyberspace, simultaneous with the development of the Internet and information-communication technology (ICT) just at the turn of 20/21 century.

In 1995, John A. Warden III has classified the cyberspace as the 5th war dimension, alongside land, sea, air an cosmic space (Figure 6).

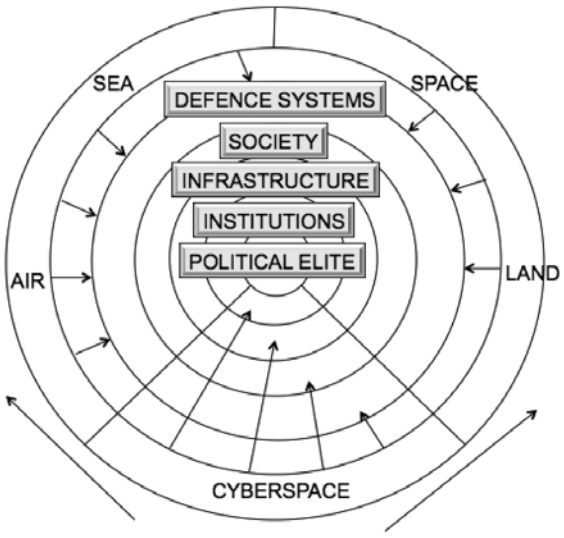

Fig. 6. Model of "five war dimensions" by J.A. Warden

Source: Sienkiewicz: 375.

In general sense, cyberspace means „world of information created by the Internet" or otherwise „communication space created by the Internet links system" (Słownik) or „electronic medium of computer networks in on-line communication" (The Free Dictionary).

American National Security Presidential Directive 54 and Homeland Security Presidential Directive 23 (NSPD-54/HSPD23) treat cyberspace as a wide-ranging infrastructure network of the information technology (the so-called "new media" – Dr. RB) (Bógdał-Brzezińska & Gawrycki 2003), covering the outside of the Internet also telecomunication networks, computer systems and variety of processors and controllers, closely related to the critical infrastructure of the State - called *Supervisory Control And Data Aquisition* (SCADA) (Assuring a Trusted and Resilient Information ; The National Strategy To Secure Cyberspace 2003).

The governmental programme of protection of cyberspace of the Republic of Poland for the years 2009-2011 defines the concept of cyberspace as a " communication space created by the system of all Internet links within the State", included the information systems, networks and services particularly significant for the State's internal security as well as banking, transport, communication, energy and water supply, health protection and other systems, which destroy or damage could pose a threat to the life or health of humans, heritage and environment or cause serious material damage (Rządowy 2009, p.4).

In conclusion it seems pertinent to **an understanding of the cyberspace** *in general sense as the all links in the sector of human activity involving Information and Communication Technologies (ICT)* (Bógdał-Brzezińska, Gawrycki 2003). So the range of cyberspace are therefore two dimensions – "human" and "technical", which – how notes Pierre Levy – can make it " the main information channel and master of the humanity's media databse" (Cyberprzestrzeń). In this sense, Daniel Solove from George Washington University believes in the total and permanent archiving of data, which is running today and threat the individual person's reputation (Heuer 2011).

Report of the Director of the Intelligence Community of the United States, Dennis C. Blair points to the two main trends in the development of information and communication technologies, which significantly affect the increase in threats in cyberspace (Blair 2010):

network convergence – the process of crossing in cyberspace of various technologies (speech processing, audio, video, computer data, Internet, etc.)

channel consolidation – the data concentration, particularly sensitive data about individual users of cyberspace obtained by various cyberaggressor for their own purposes.

Some researcher also point to the fact, that cyberspace is **virtual in nature**, so there is no traditional geographical parameter and associated with its limited to the fullest dimension. The framework and the limits of cyberspace define the continously variable level of current development of the information technology and the degree of networking of the world. In this sense, it says even about the "death of distance". This approach makes cyberspace the unmeasurable and unlimited object, "(...) space without place, space in which the various sphere and plan overlap, penetrate, intersect" (Słownik).

Another important feature of the cyberspace is also its specific **"monocultural"** as the result of the progressive integration of the information and communication systems and the common use of the same or similar and compatible technical solutions, and in particular the software, what a good illustration is the dominance of specific operationg systems. "This trend has its economic background and is conductive to their further development, expanding coverage and increasing the operation's efficiency (taking under consideration the optimization of the operation requirements of the complex systems – unifying the rules and procedures of the framework). However, it has the serious implications in the sphere of security, increasing the system nature of risk of possible negative consequences of the attacks and accidents and the possibility of their cascade spread in the so unified network" (Madej 2009).

At the same time, there is a process of the progressive **nationalisation of cyberspace**, which should not confused with another also important phenomenon, which is cybernationalism, i.e. nationalism in cyberspace. A growing number of States and also non-State actors already perceive the cyberspace as the new reach "continent" (space) to win and explore. For example, the Russian Federation had been implemented the Operating Investigative System (SORM-2) to copy every bit of information that enters or leaves its country's information and communication systems into the great server managed by the Russian Federal Security Service (FSB). China is managing the "great firewall" filtering politically incorrect websites, as well as pornography and other forms of the "cultural plague". The United States has transferred control of the language and domain names on the Internet to the *non profit* organization Icann, which is transforming into a supervisory body modelled on the United Nations (UN) now.

"China will soon have absolute authority over the network's structure within their borders. The legal map of cyberspace in the West is more chaotic. However, we are the witnesses of creating thousands of laws and regulations by parliaments and courts" (Glenny). Without a doubt, there is an urgent need **to define the policy managament of the cyberspace**. Emerging already in this respect, the ad hoc arrangements characterise the lack of a coherent strategy and the traditional tools developing by States the world order in the 19th century, such as the law and treaties, have

occured insufficient (if not completely irrelevent) in relation to the new domain.

Outlined above features of cyberspace are of course only exemplary and in no way cover all of the above issues, indicating however its complexity, multiaspect and the sources of the not yet explained or even identified phenomenons the existance we will see with time. For the natural reasons, such environment is the generator of the phenomenons of both positive, foster the development of humanity, and nagative, as the threat on the unforeseen range.

4. Cyberthreats: attempt of conceptual analysis

The main challenges and threats in cyberspace include (Figure 7):

- information warfare
- cyberterrorism
- cybercrime
- cyberespionage.

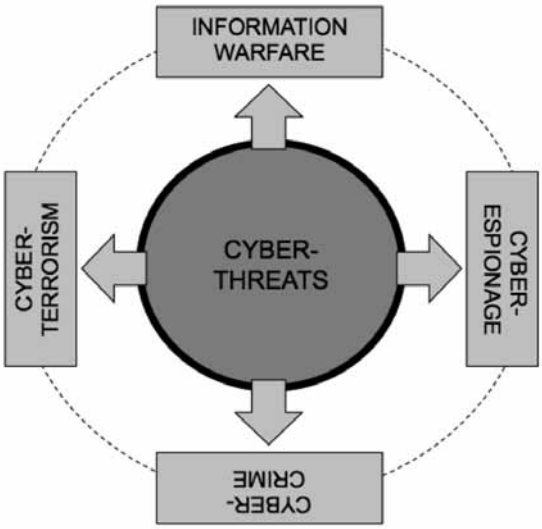

Fig. 7. The main challenges and threats in cyberspace

Source: Author.

An effort on defining those terms are undertaken in the literature now. In this respect there is a great diversity of approaches. This same concept are often assignied different meanings, which indeed makes it difficult to identity them and prevent their impacts on the security environment.

This can be explained by the example of the selected definition concepts of war information and cyberterrorism.

The term of information warfare (IW or iWar) firstly has appeared in the military terminology due to scientific and technological progress. Among the many definitions formulated by the Polish scientifict researchers, the concept of Ryszard Szpyra seems to be very interesting. He sees the information warfare as "the organised in the form of violence, the military external activity of State to achieve certain political purposes, aimed at destroying or modifying information-communication systems or transmiting information of the enemy as well as the protection activities of their own systems and information from the similar enemy's response action" (Pawłowski 2002).

This approach is both offensive and defensive sense, reflected also in the other concepts. For example, the US Defense Department specifies information warfare as " an actions aimed at achieving information superiority through the impact on enemy's information, information systems, transmitting process and computer networks and defending its own information, information systems, transmitting process and computer networks" (Hildreth 2001).

However, some definitions of information warfare are very close to meaning of cyberterrorism presented by some researchers.

An example is the concept of information warfare developed by Alan D. Campen, which specifically refers to the non-military aspect of issue, which can be seen as "(...) manipulative and disruptive actions, conducted from the hide, or expicitly in time of peace, crisis and war, directed on electronic information systems, with the objective of social, political, or economic" (Bógdał-Brzezińska, Gawrycki 2003).

Hence is the close, for example, to the definition of cyberterrorism according to D. Verton as " politically substantiated and reasoned the activities of groups of national or other enemy forces targeted against information, computer systems, programs and data, which impact on the non-military targets, carried out by ethnic groups or secret agents" (Pollit).

Similarly ambiguous is the concept of cybercrime. For example the Council of Europe Convention on cybercrime refers to four types of crimes, without indicating the offender, his motivations and effects (Kosiński, Kmiotek):

- the traditional form of crime, such as fraud or forgery, which in the context of cybercrime, concern crimes committed using electronic information networks and information systems

- the publication of illegal content in electronic media (e.g. materials related to the sexual utilization of children, or the calling to the hate racial)
- the crimes typical for electronic communications networks as: attacks against information systems, e.g. DoS (denial of service), hacking, pharming, violation of the integrity of information systems, etc. It should be noted that such attacks also can be directed against the most elements of the critical infrastructure in Europe and damage the existing rapid response systems in many areas, which may cause the dramatic consequences for the society
- „digital" reproduction and dissemination of artistic works or performances without the consent of the entitled person to benefits.

In principle, the concept of cyberespionage is not explicity defined in literature and refers to the general concept of espionage as an activity of getting a secret information for the purposes of the foreign intelligence.

In most countries, the espionage on the behalf of a foreign country is a criminal act the highest penalities. For example the Polish Penal Code as one of the types of certified espionage recognises:

collect or store messages or illegal breaking information system to obtain it an grant foreign intelligence or notification of readiness for foreign intelligence against the Republic of Poland (article 130 § 3 pc) is treated as a crime threatned deprivation of liberty from 6 months to 8 years (Ustawa).

A characteristic feature of an espionage is the secret activity (conspiracy character) and the use of methods and techniques of intelligence, which also should be concerned to the concept of cyberespionage.

In conclusion, it should be noted that:

in the ongoing process of defining the cyberthreats we are dealing with **overlaps their conceptual space**.

Therefore, some researchers are looking for determinants (i.e. defining factors), which in a suffieciently distinct way would allow the distinction between the various types of cyberthreats and this way to avoid some major problems and perturbation. And this approach seems correct.

The proposal of Rod Stark is a good example of this way of thinking. For the principle criterion of distniction between the information warfare and cyberterrorism (CT) he takes **the factor of attacking subject (attacker)**. He argues that if an attacker (cyberaggressor) is the State subject (actor), we are dealing with the iWar. In case, when the attacker is non-State actor, we are dealing with cyberterrorism. In addition, Stark notes that in the case of information warfare States are going to get the information dominance over its opponent (enemy), that must not get in the case of cyberterrorist actions, which additional have a spontaneous and separated character, while the iWar states a part of the wider military operations (Bógdał-Brzezińska, Gawrycki 2003).

However the concept of Stark mainly based on the attacker factor seems insufficient, even in a view of fact, that in the event of iWar we have to deal with the use by State actors the non-State actors as intermediaries whether the mercenaries, and cyberattackers may also be supported it State actors (sponsors), as in the case of classical terrorism.

Additionally, non-state actors may also be the cyberattackers and generate the acts of cyberespionage (Figure 8).

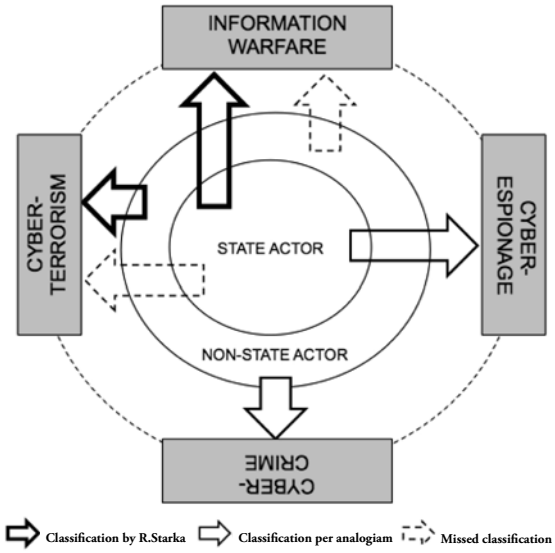

Fig. 8. Cyberthreats concept by Rod Stark based on the cyberattacker factor
Source: Author.

This criterion seems to be indispensable as scarce to identify categories of cyberthreats and in this regard should be sought more advanced solutions.

Some proposal, may be presented by me the concept of cyberthreats typology based on four factors (Figure 9) (Białoskórski 2011a):
1) attacking subject (cyberattacker, cyberaggressor)
2) attacked subject (cybervictim)
3) purpose/motivation of attack

4) result (effect) of attack.

According to this concept, the definition of the various categories of cyberthreats provides as follows:

- **information warfare (iWar)** – various actions in cyberspace inspired and directly or indirectly conducted by States and/or international organizations *(attacking subject)* directed against other States, international organizations and/or non-State actors *(attacked subject)*, which directly or indirectly lead to injure or death people and damage or destroy the elements of critical infrastructure *(result)*, in order to achieve the State's national interests or the interests of the organization *(purpose/motivation)*
- **cyberterrorism (CT)** – various politically or ideologically motivated *(purpose/motivation)* terrorist actions or their intention in cyberspace to be conducted by individuals (persons) or terrorist organizations *(attacking subject)* directed against States, international organizations or transnational objects *(attacked subject)*, which directly or indirectly lead or may lead to injure or death people and damage or destroy the elements of critical infrastructure *(result)*
- **cybercrime (CC)** – financially or materially motiveted *(purpose/motivation)* actions or their intention in cyberspace to be conducted by individuals (persons) or international criminal groups *(attacking subject)* directed against various State and non-State subjetcs *(attacked subject)*, which directly or indirectly lead or may lead to some financial and/or material losses *(result)*
- **cyberespionage (CE)** – process of getting the intelligence information and/or materials *(result)* i.e. presenting important value from the intelligence tasks point of view *(purpose/motivation)* carried out by the intelligence service *(attacking subject)* be placed into cyberspace in the disposal of any subject which remains in spyware interest *(attacked subject)* with using of miscellaneous intelligence methods and techniques, particularly cyber.

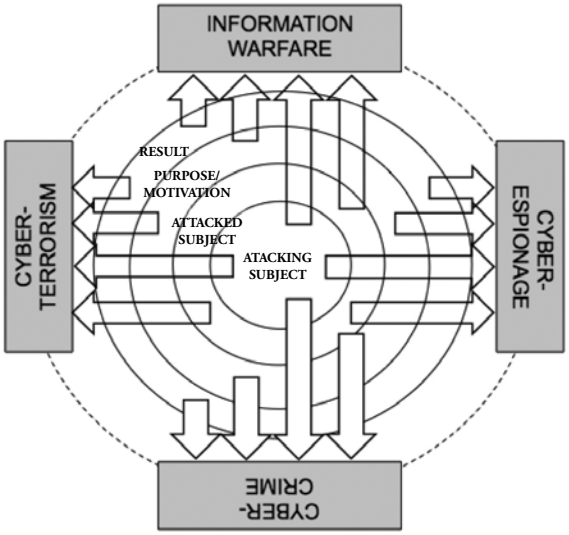

Fig. 9. Cyberthreats concept by Robert Białoskórski based on the analysis of four factors
Source: Author.

Table 1 presents a summary description of the components of each of four factors related to the individual types of cyberthreats.

Table 1. Description of the analysis factors of cyberthreats by Robert Białoskórski concept

STIPULATING FACTOR / CYBERTHREAT	ATTACKING SUBJECT	ATTACKED SUBJECT	PURPOSE/ MOTIVATION	RESULT
INFORMATION WARFARE	States/IO's	States/IO's/TNO's/ ITO's/ICG's	National interest/ organization interest	Injuring or killing people and damaging or destroying the elements of critical infrastructure
CYBERTERRORISM	ITO's/individuals (persons)	States/IO's/TNO's	Political/ideological	Injuring or killing people and damaging or destroying the elements of critical infrastructure
CYBERCRIME	ICG's/individuals (persons)	States/IO's/TNO's/ individuals (persons)	Financial/material	Financial/material losses
CYBERESPIONAGE	States (inteligent services)	States/IO's/TNO's/ ITO's/individuals (persons)	Intelligence	Getting the intelligence information and/ or materials

Source: Author *(Legend: IO's - International Organizations, TNO's - Transnational Objects, ITO's – International Terrorist Organizations, ICG's – International Criminal Groups).*

It seems that such multivectors approach to the presented issue enables more unequivocal categoriziation of cyberthreats.

This can be illustrated by the example of the cyberattack in Iran using the virus "stuxnet" in 2010.

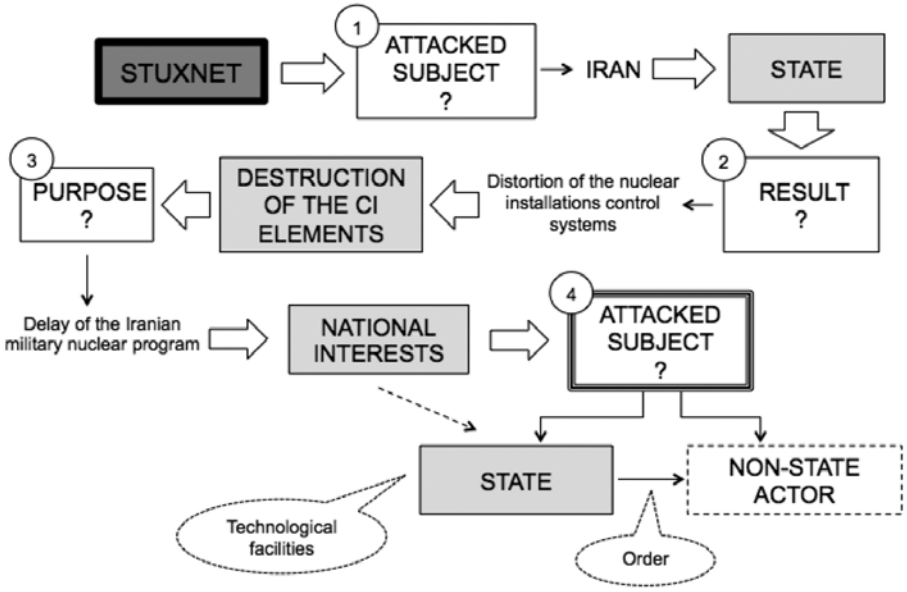

Fig. 10. An example of cyberthreats analysis (stuxnet case-study)
Source: Author.

Attacked subject to take in this case is primarily Iran, because of the largest percentage of the number of infected systems, the virus Stuxnet (58,31%), next in Indonesia (17,83%) and India (9,96%) (Falliere, Murchu, Chien 2010). Similarly, the result of cyberattack do not raises doubts, since it has caused disruption in Iranian nuclear instalations systems which are the elements of critical infrastructur (CI). The purpose of this cyberattack is also clearly, delay of Iranian nuclear program, which is suspected also to be the military nature. Such purpose can only be by States articulated, driven by specific national interests (David, Brannan, Walrond, 2010).

In the presented concept, the greatest difficulty makes the determination of the attacking subject (cyberattacker), particularly in situation, when it acts secret and does not admit for cyberattack. In the stuxnet case, it semms relatively easy, mainly for two reasons: the purpose of attack (i.e. national interest) and the necessary technological advancing. It seems indeed, that presently only the State or States (Israel and the United States are mostly suspected) may be cyberaggressors. In the future, it should be taken into consideration that, in the situation of proliferation of advanced iWar's technology, one of the State actors, according to its particular national interest, may have order the execution of cyberattack, e.g. international terrorist organization (as already mentioned, we have indeed now in the security environment to deal also with States sponsoring terrorism or even permit are acts of terror). Then, the determination of the employer, *de facto* the attackig subject can pose a big problem.

Finally, in the case of stuxnet, this kind of cyberattack can be recognized as the cyberwarfare (iWar), and more specifically from the military strategic point of view as the information operation.

5. Conclusions

Presented in the paper attempt of multivectors analysis of the conceptual model of the principle cyberthreats in the context of the new security environment approach results mainly from the need of their distinct discrimination to take optimum preventive and counteract actions.

The author hopes, that it will provide the scientific inspiration to search and develop other alternatives approaches of this problem in a circle of interested researchers.

References

A Secure Europe in a better world. European Security Strategy, 2003. Available from http://consilium.europa.eu/uedocs/cmsUpload/78367.pdf (15 May 2012).

Albright, David & Brannan Paul & Walrond Christina. 2010. Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant', Institute for Science and International Security Report. Available

from http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf (15 May 2012).

Assuring a Trusted and Resilient Information and Communications Infrastructure, *Cyberspace Policy Review*. Available from http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (15 May 2012).

Białoskórski, R. 2011a. *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki* [The Cybersecurity in the Security Environment of the 21st Century. An outline of issues]. Warszawa: WSCIL.

Białoskórski, R. 2011b. 'Czynnik informacyjny warunkiem sine gua non procesu conflict prevention' [Information Factor as the Sine Qua Non Condition of the Conflict Prevention Process], in Wiesław Stach, ed., *Bezpieczeństwo współczesnego świata - polskie aspekty i uwarunkowania* [The Security of Modern World – Polish Aspects and Considerations]. Poznań: WSHiU (15-32).

Białoskórski, R. 2011c. 'Koncepcja Conflict Prevention. Zarys problemu badawczego' [The Concept of Conflict Prevention. An Outline of the Research Problem], in: Wojciech Kostecki, ed., *Zaawansowane zapobieganie konfliktom* [The Advanced Conflict Prevention]. Warszawa: ASPRA JR (97-106).

Białoskórski, R. 2010. *Wyzwania i zagrożenia bezpieczeństwa XXI wieku* [The Challenges and Threats of Security 21St Century]. Warszawa: WSCiL.

Blair, D. C. 2010. 'Annual Treat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence', Council on Foreign Relations. Availabe from http://www.cfr.org/intelligence/annual-threat-assessment-intelligence-community-senate-select-committee-intelligence-2010/p21369 (15 May 2012).

Bógdał-Brzezińska, A.; Gawrycki, M. F. 2003. *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie* [Cyberterrorism and the Information Security Problems in The Modern World]. Warszawa: ASPRA-JR.

Cyberprzestrzeń – definicje [Cyberthreats - definitions]. Available from http://www.techsty.art.pl/hipertekst/cyberprzestrzen.htm (15 May 2012).

Department of Defence Strategy for Operating in Cyberspace, 2011; available at http://www.defense.gov/news/d20110714cyber.pdf (15 May 2012).

Falliere, N.; Murchu, L. O.; Chien, E. 2010. W32. Stuxnet. Available from http://securityresponse.symantec.com/en/id/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (15 May 2012).

Glenny, M. Nacjonalizacja cyberprzestrzeni przebiega w coraz szybszym tempie. [Nationalization of cyberspace is in an increasingly faster pace]; available at http://forsal.pl/artykuly/409450,nacjonalizacja_cyberprzestrzeni_przebiega_w_coraz_szybszym_tempie.html (15 May 2012).

Heuer, S. 2011. 'Ile bitów tyle kłamstw' [How many bits behind the lies], *Forum*, No. 13.

Hildreth, S. A. 2001. Cyberwarfare, CRS Report for Congress, Washington D.C.. Available from http://www.fas.org/irp/crs/RL30735.pdf (15 May 2012).

Kosiński, J.; Kmiotek, S. 'Międzynarodowa współpraca w zwalczaniu cyberprzestępczości' [International Cooperation in The Fight Against Cybercrime]; available at http://www.dobrauczelnia.pl/upload/File/KONFERENCJE/Cyberrteroryzm/kosinski_kmiotek.pdf (15 May 2012).

Koziej, S. 2010. 'Strategiczne środowisko bezpieczeństwa międzynarodowego i narodowego w okresie pozimnowojennym' [National and International Strategic Security Environment in the post cold war period]. Available from http://www.koziej.pl/index.php?pid=5 (15 May 2012).

Lasoń, M. 2010. Bezpieczeństwo w stosunkach międzynarodowych [Security in The International Relations], in Erhard Cziomer, ed., *Bezpieczeństwo międzynarodowe w XXI wieku. Wybrane problemy* [International Security in 21st Century. Selected Problems]. Kraków: Krakowskie Towarzystwo Edukacyjne – AFM (9-32).

Madej, M. 2009. 'Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego' [Revolution in Informatics – Gist, Manifestations and The Impact on Perception of Security of States and The International System, in: Marek Madej & Marcin Terlikowski, ed., *Bezpieczeństwo teleinformatyczne państwa* [The Teleinformation Security of State]. Warszawa: PISM (17-40).

NATO 2020: Assured Security; Dynamic Engagement, 2010. Available from http://www.nato.int/cps/en/natolive/official_texts_63654.htm (15 May 2012).

Olchowski, J.; Pietraś, M. (eds), 2011. NATO w pozimnowojennym środowisku (nie)bezpieczeństwa [NATO in The Post Cold War (In)Security Environment]. Lublin: UMCS.

Pawłowski, J. (ed.). 2002. *Słownik terminów z zakresu bezpieczeństwa narodowego* [Dictionary of national security terms]. Warszawa: AON.

Pollitt, M. M. Cyberterrorism - Fact or Fancy? Available from http://www.cs.georgetown.edu/~denning/infosec/pollitt.html (15 May 2012).

Rotfeld, Adam D, 2006. *Polska w niepewnym świecie* [Poland in an Uncertain World], Warszawa: PISM.

Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011 – założenia [The Governmental Programme of Protection of Cyberspace of Republic of Poland for the years 2009-2011 – assumptions]. Available from http://www.cert.gov.pl/portal/cer/30/23/Rzadowy_program_ochrony_cyberprzestrzeni_RP_na_lata_20092011__zalozenia.html (15 April 2012).

Sienkiewicz, P. Wizje i modele wojny informacyjnej [Visions and models of information war]. Available from http://winntbg.bg.agh.edu.pl/skrypty2/0095/373-378.pdf (1 March 2012).

Słownik slangu informatycznego [Dictionary of Computer Slang]. Available from http://www.islownik.pl/1,323,cyberprzestrzen.html (15 May 2012).

The Free Dictionary; available at http://www.thefreedictionary.com/cyberspace (15 May 2012).

The National Strategy To Secure Cyberspace, 2003. Available from http://georgewbush-whitehouse.archives.gov/pcipb/cyberspace_strategy.pdf (14 April 2011).

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny [The Act of June 6, 1997. Penal Code]. Available from http://isap.sejm.gov.pl/DetailsServlet?id=WDU19970880553 (15 May 2012).

Verton, D.; Ice, B. 2004. *Niewidzialna groźba cyberterroryzmu* [The Invisible Threat of Cyberterrorism], Gliwice: Helion.

Ziarko, Janusz, 2007. 'Uwagi o przedmiocie nauki o bezpieczeństwie' [Remarks on the subject of security science], *Problemy bezpieczeństwa* [Security Problems], Czasopismo Krakowskiej Szkoły Wyższej, No. 1.

Żukrowska, K.; Grącik, M. 2005. *Bezpieczeństwo międzynarodowe. Teoria i praktyka* [International Security. Theory and Practice], Warszawa: SGH.