SELECTED MODELS OF INFORMATION WARFARE IN CYBERSPACE

Lt. Col. Radosław BIELAWSKI, PhD Eng.
War Studies University, Warsaw, Poland
r.bielawski@akademia.mil.pl

Aleksandra RADOMSKA
War Studies University, Warsaw, Poland
aleksandra650@gmail.com

Introduction

One form of activity in cyberspace is the information battle. One of the proposed definitions will define it as a negative co–operation in the sphere of information acquisition, information distortion and information defense, where each side of the action is subordinated to the antagonistic side of the other[1]*. It leads to the achievement of political objectives and is aimed at overthrowing the systems of the state responsible for the state of its security. It is important that this condition is at a high, or at least acceptable, level. To ensure this level, it is important to define cybersecurity fighting models that are adequate for the threats and to determine their impact on the level of national security risk in cyberspace. Literature on the subject contains many models of cyberwarfare information that have been shaped in recent years. However, there is no assessment of the adequacy of these models for the risks and risks associated with national security threats. It should be noted that information security itself, as part of national security, is variable. New threats are emerging and, at a very high rate and with high activity in cyberspace, they are capable of destabilising the security of key state administration bodies, military facilities and other important state–run infrastructures.*

It should be emphasised that existing cyberspace fighting information models are not universal and cannot be used for any type of threat to national security. They need to find, organise and evaluate those that would be the most appropriate not only for national

1 L. Ciborowski, *Walka informacyjna*, Adam Marszałek, Toruń, 1999, p. 187.

security threats but also for geopolitical determinants. Assumptions for the research and its results are a noticeable increase in the number of cyberattacks, some of which are important from the point of view of national security – the military system and critical infrastructure elements of the state.

The following subject of the research was adopted in the article – models of information fight, related to threats to national security coming from / to cyberspace. The purpose of scientific research is to define models of information combat and to determine the suitability and evaluation of these models for the purpose of evaluating the risks of national security threats. Identifying the subject and objectives of the research led to a general research question: ***What appropriate models of information fight in cyberspace can be defined and used for the risks of national security threats?*** *The research method applied theoretical methods (analysis, synthesis, generalisation, abstraction, inference, analogy and comparison) as well as the empirical method of dialogue and the method of participant observation.*

Key words: cyberspace, information models, national security, military system, critical infrastructure

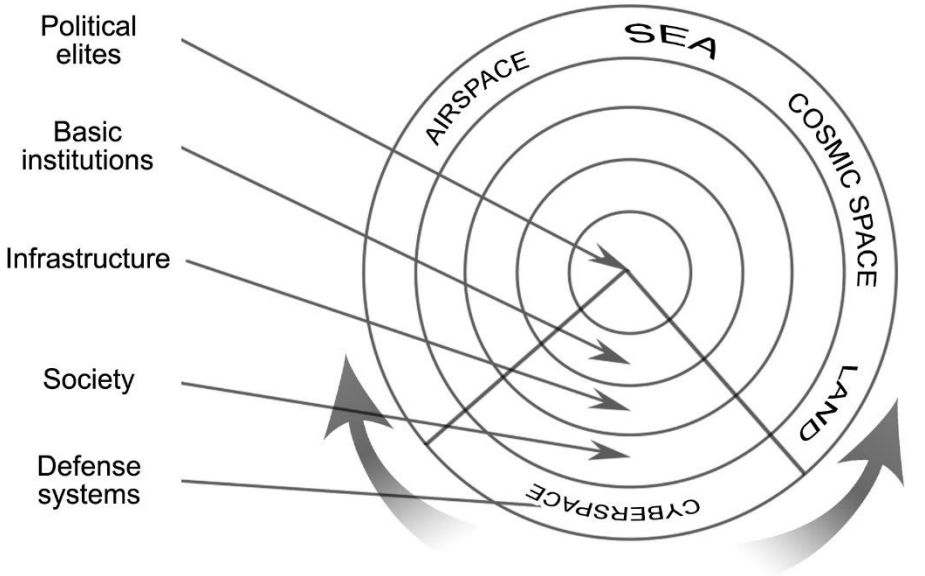
The Decapitation Theory and The Warden Model

A basic, yet universal, tool for examining the course of any contemporary conflict is the concept developed by Colonel John Warden[2]. It is known as the „five dimensions", „five circles" or „five rings" (Figure 1) defined by Warden based on the experiences of the Gulf War[3], and in the domestic literature of the information war continued by Professor Piotr Sienkiewicz[4]. It implies the existence of five dimensions through which it is possible to influence the opponent. They are: land, sea, air space, space and cyber space.

2 J. Warden, *The Enemy as System, Maxwell 1995*, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm [accessed: 23.04.2017].

3 W. Krautz, *Piąty wymiar walki, czyli logiczne konsekwencje modelu Wardena*, http://xportal.pl/?p=2110 [accessed: 28.06.2017].

4 P. Sienkiewicz, *Wizje i modele wojny informacyjnej* [in:] *Społeczeństwo informacyjne – wizja czy rzeczywistość?, Main Library of AGH University of Science and Technology*, Cracow, 2003, p. 375.



Source: my own work based on P. Sienkiewicz, *Visions and models of war*..., op. cit., p. 375.

Fig. 1. The "five dimensions" of a battle according to Warden

According to Warden's theory, the opponent is understood as a system and has been compared to the functioning of the human organism. It consists of interrelated circles that perform complex roles that form the systemic whole of an organisation, state, criminal gang, or organised terrorist group. The enemy side was defined as:

- **defence systems** – defined as a component of actors, which include all the forces and means used to defend the state from the enemy, such as the armed forces and other services such as the police, the guard (e.g. border);
- **society** – defined as population, demographic groups, classes and social elites;
- **infrastructure** – defined as the critical infrastructure of the state, the physical elements that determine its existence and the smooth functioning of a given activity, e.g. roads, airports, factories;
- **basic institutions** – defined as a component in which processes to meet the needs of the organic population, such as electricity, gas, water, oil, cash resources, food supplies,

– **political elite** – defined as a component of the highest level of leadership, leadership, or command at strategic level, e.g. in the case of the functioning of the state, it may be the government[5].

The theory is that defence systems recognised as the first outer circle can be destroyed using a variety of military means from each space in addition to the cybernetic environment. Cyberspace, due to the characteristics that distinguish it, can penetrate the other rings, causing destructive impact on the opponent. It is a „field of information war", allowing for free circulation of information. All of the activities that comprise the essence of information conflicts can be divided into offensive (defensive) and defensive (targeted towards the planned attack) and deemed necessary to achieve the desired advantage in the information area over the opponent. Its purpose is to achieve the intended political priorities. With regard to the information presented in the framework of the Information Fight, one can distinguish two basic assumptions which lead to:
– destroying the impact and degradation of the information resources of the opposite party and any information systems used by it;
– guaranteeing the security of their own resources and information systems, eliminating the likelihood of cyberattacks on them[6].

Dugin's Eurasian and Atlantic Model

In order to understand the Eurasian model of information struggle, it is necessary to first understand the essence of the ideological movement, which is promoted by Alexander Dugin, the Russian historian of religion, philosopher, journalist and international affairs expert. His theory is based on geopolitical considerations. Their genesis is a fundamental work in this field. *The Geographic Axis of History* by Halford Mackinder. It is a collection of reflections on the relationships between geography, history and politics. In Mackinder's paper, Mackinder assumes that the natural environment is to be under the absolute control of man, although

5 W. Scheffs, *Automatyzacja działań urządzeń elektronicznych w środowisku cyberprzestrzeni i walki elektronicznej*, Journal of KONBiN, 2011, 3(19), p. 127.
6 P. Sienkiewicz, *Wizje i modele wojny…*, op. cit. , p. 375.

ultimately this relationship turns out to be mutual. The continents are small islands in the universe of the ocean. According to Mackinder, land control provides control and dominance over the sea. The key to global policy from the European perspective is the Eurasian region of the Great Steppe, which the author calls Heartland (the heart of the continent). Heartland covers the territory of the north–eastern part of the Eurasian continent; It is a belt of forests and steppes, stretching from Poland and Hungary to Mongolia. Dominating the Island of Europe (Europe–Asia–North Africa) and, according to the Geographic Centre of History, gives you unparalleled control over the entire planet from the mainland. Based on the above assumptions, Dugin made an authoritative approach to the geopolitical aspects of Russia. First and foremost, the motif in his publications is the need to expand the political and military influence of the country. He contends, like Mackinder, that gaining control of Heartland can bring enormous geopolitical benefits. He identifies him with the greatest powers, including the territories of the Russian Empire, the Union of Soviet Socialist Republics and the current Russian Federation[7]. On this basis, he believes that Russia should at all times strive to maintain control and control in this part of the world. Dugin in his thesis notes the existence of power, threatening the rule of land. He recognises it as a civilization that has been naturally shaped to compete for and confront directly with the Eastern powers. He defines it as *Sea Power*, identified with the power of the western hemisphere, that is, the United States. Alexander Dugin states that both civilizations are two hostile camps located on opposite sides of the world. This means that the "power of the sea"[8] (the West) is symmetrically opposed to the „power of the land"[9] (East). Broadly understood strategies of these states are divided by their ideologies. The subordinate areas of Eurasia recognise the values to which they are classified:

– **collectivism** – a view that emphasises the importance of communities and communities in society. Collectivism is the opposite of national individualism

7 Ibid.

8 Talassocracy – the term from ancient Greek, relating to countries wielding power at the sea. Thanks to the desired domination at the sea, they also have power on the land. Contemporary talassocracy means sea domination in the aspects of economy, economics, or the military.

9 Tellurocracy – the term from ancient Greek, relating to countries wielding power and control on the land. Contemporary tellurocracy means land in the aspects of economy, economics, or the military.

in the context of an individual's view. Consequently, this value calls for the promotion of goals and good for groups;
- **solidarity in interpersonal relations** – a view derived directly from the idea of collectivism, referring to deep bonds in a particular community. It also means the unification of individuals from the same nationality;
- **tradition** – that is, the view that, based on the transmitted content of culture, a specific social group that recognises the values as important and necessary for the development of their country and its future. Culture in this case includes: beliefs, views, way of thinking, behaviour, social norms;
- **spiritual values**.

Sea Power, as a counterweight to the Eurasian territories, professes quite different views on the basis of which Western civilization was born. Dugin defined it as Atlantic areas, built in harmony with the Roman patterns prevailing on them based on Catholic and Protestant religions. The values of the Atlantic are:
- **individualism** – the opposite of collectivism, widespread and highly valued in the Eurasian territories. A view that accepts the human individual as the highest good in society, and fulfills its needs as the overriding issue;
- **liberalism** – ideology and political direction, promoting broadly understood freedom as the greatest value. Its characteristic features are individualism, opposing collectivism, belief in equality, tolerance, autonomy, individual freedom, bodily integrity, and political pluralism;
- **capitalism** – the system of functioning of the economy of the country, based on the private ownership of means of production, which ultimately can be profitable. Capitalism also involves unrestricted free trade in goods;
- **materialism** is an attitude that is related to the development of capitalism. It means that a person is completely focused on material values such as money, finances and profits. The person who represents such a position is not interested in social bonds and building solidarity in relations between people;
- **globalism** – a set of beliefs about the process of globalisation, based on the view of global prosperity, the emancipation of individuals, the spread of values (e.g. human rights), and the world becoming significantly (to a large extent positive);
- **technocracy** – the concept of a social system in which authority and senior positions would be made by experts with specialist knowledge in a specific field of study or economy of exceptional importance for the proper functioning of

the state. Technocrats believe that the concept promoted by them can influence changes in the social and cultural spheres. In the social sphere, it guarantees professionalism on the basis of "experts–species", guided by the motives of the best solution of various matters. In the cultural sphere, it offers some degree of self–improvement to individuals. According to the ideology of technocratism, scientific knowledge is only available to a small group of people.

According to the assumptions set by Alexander Dugin, Russia has the appropriate predisposition to become the world's largest land power, identified in the first geopolitical concepts with Heartland. However, the power of West Power, the Atlantic civilisation identified with the United States, remains a precondition for this power.

Taking into account the theses that are based on philosophical ideologies and geopolitical determinants, we can show a varied circulation of information used in the above superpowers – the United States and Russia. The American war in cyber space is network–centric (net–centric warfare). In the simplest sense, the concept of the cybersecurity information field is a platform for fast and efficient exchange of information, most often for the benefit of the military, using advanced electronic devices. This solution aims to provide the desired advantage over the opponent by distributing data regardless of geographic location. In terms of the use of cybernetics for the needs of US troops, it also includes:

– creating a new information infrastructure for the armed forces;
– interactive components, compatible with infrastructure resources;
– very fast links, allowing for coordinated data flow.

Based on United States' strengths and measures, Dugin states that the actions they take are based primarily on advanced technology and trained IT specialists with knowledge of the effective use of their resources. This enables them to gain an information advantage, delivered in real time, to increase combat capability by distributing it to all potential customers. The Atlantic Battle Network model is defined as an artificial process that increases the enemy's demand for information and limits the enemy's access to it while providing the widest possible access to data, using network mechanisms and feedback tools, while protecting the troops from the enemy[10].

10 A. Dugin, *Gieopolitikapostmoderna*, (trans.) P. Sieradzan, Geopolityka, 1(2), 2009.

In order to gain an advantage over it, Dugin issued a forecast for the development and modernisation of Russian resources, defining the Eurasian model he developed for the first time. The Russian theory of information wars can be described as an example of interdisciplinary applied science. It refers to a very wide range of actions aimed at attaining the intended political, economic, social, military, intelligence, counterintelligence, diplomatic, propaganda, psychological, information and educational purposes[11]. With the desire to match the US–based network of cyberspace, Dugin is expected to set up a staff of high officials, intellectuals, special services, political scientists, academics, cultural activists and patriotic–oriented journalists. In this way, the effect of combining the elements of the cyano–centric approach, which is prevalent in the „postmodern" West with the Russian specifics of the fight against information[12], will be possible. It is defined as a phenomenon focused on mass consciousness in the interstate rivalry of civilisational systems in cyberspace, using particular means of controlling information resources and being used as **information weapons**[13]. For the Eurasian model to be effective, modernisation of all Russian institutions, organisations, services and network and communication lines must be carried out. This means that information vectors of symmetrically aligned models would be directed in opposite directions of network destruction.

Panarin's Information Fight Model

Another example of a pattern of information warfare is a model developed by a political scientist and professor at the Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation, Igor Panarin. He based his theory on the basis of the need to actively counter Russia against the United States in the context of information operations. There are two events that are significant

11 M. Orzechowski, *Koncepcja walki informacyjnej jako element bezpieczeństwa Federacji Rosyjskiej. Wojna w Donbasie jako study case zastosowania elementów walki informacyjnej* [in:] *Polska – Rosja, Polityka bezpieczeństwa Federacji Rosyjskiej*, ed. M. Kaszub, M. Minkin, Wydawnictwo UPH, Siedlce, 2016, p. 105.

12 J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*, OSW, Warsaw, 2014, pp. 17–18.

13 M. Orzechowski, *Koncepcja walki informacyjnej…*, op. cit.

for the Russian Federation, which define the expression of the aggression of the West. There is a ring that ended in the break–up of the Union of Soviet Socialist Republics in 1991, considered to be the largest contemporary land power in the world, and rivalry (among other things in technological advances) that began at the beginning of the present millennium. According to forecasts by prof. Panarin, this will end in 2020 with the domination of Dobra, which is the advantage of the Russian Eurasian model over the American Atlantic model[14].

Igor Panarin assumes that contemporary information attacks are an initiative of the United States alone to control the public using their own highly–developed information aggression tools. Like Aleksandr Dugin, they define them as artificial processes, based solely on highly advanced technical means. In his work, he distinguishes three aspects of cyberwarfare, in line with Dugin's assumptions in the context of the Russian Information War, as a weapon of human consciousness perceived by the surrounding reality. As a first aspect, prof. Panarin defines actions that are in fact actual impact operations, which include:

– **social control** – it is a conscious effort to influence the behaviour or way of thinking of a community, with the aim of achieving specific goals. In the context of information, social control means influencing people's cognitive processes, emotions, motivations or shaping persistent attitudes through selective control of information flow, for example, by encouraging positive and negative prejudices, targeting interests, informing the shape of desired public acceptance;
– **social maneuvering** – this is an intentional form of controlling individuals to achieve the intended benefits. Social maneuvering strives to subordinate itself to a certain population of citizens of a given state by the opponent (e.g. a hostile country) defined as an information aggressor. With the help of the acquired groups, the information aggressor can take control over the resources and structures of the country that is the cyberattack object;
– **manipulation of information** – action involving a camouflaged effect on the behaviour and awareness of individuals and social groups in order to achieve planned goals. It includes a number of techniques such as moralising (for example, prompting and warning), provocations (e.g. inducing individuals to

14 J. Darczewska, *Anatomia rosyjskiej wojny…*, op. cit., pp. 14–15.

perform an activity they would normally not have done), ridiculing people (e.g. provoking situations where the subject of manipulation is ridiculed), disseminating national or racial stereotypes (e.g., in the form of a brief picture of a group of people functioning in the consciousness of members of another group);

- **disinformation** – involves deliberately falsifying existing information and passing it on to the public to mislead. Disinformation is particularly important in the security and defence aspects of the state. An example of this might be misleading an opponent about the possession of an atomic weapon that does not exist;
- **information fabrication** – a process defined as the production of new information in order to falsify it and then disseminate it in society;
- **lobbing** – an action to influence influences by specialised advocates of interests on public authorities based on a communication strategy. Lobbing includes a structured cycle, including: decision analysis, policy of a particular authority, strategic goals, SWOT analysis, ongoing monitoring of events;
- **blackmail** – a form of criminal activity based on attempts to force a particular individual to perform a particular activity, to abandon or disclose certain (partially or wholly real) information using tools in the form of verbal threats or physical violence;
- **enforcing the desired information** – a form of criminal activity involving the use of verbal threats or physical violence to obtain information of significant and important character.

Another factor highlighted by prof. Panarin is the tool for running a Russian information war in cyberspace. Once the action has been taken, it states that appropriate measures must be taken that directly affect the collective population. Among these tools, he made a division into secret and overt and then distinguished:

- **propaganda** – one of the tools based on purposeful action to shape the minds, behaviour and way of thinking of a particular group of people, involving emotional and intellectual manipulation. The types of propaganda include: black propaganda (as a source of information to a false sender), grey propaganda (the source and source of information for the recipient remains unknown) and white propaganda (source and origin of information is credible);

– **intelligence** – defined as a special service, established for the acquisition of classified information about the enemy, dealing with its processing, storage, analysis and transfer of power;
– **analytical component** – in the context of information warfare, this is an action based on uninterrupted control of mass media while analysing the current situation or changes in the monitored environment;
– **organisational component** – in terms of information warfare, this is the whole of the management structure in the process of ongoing cybernetic operations, which can include coordination and steering channels or agents that have a special significance for information provided by the media;
– **other conjugated channels** – largely related to diversionary activities.

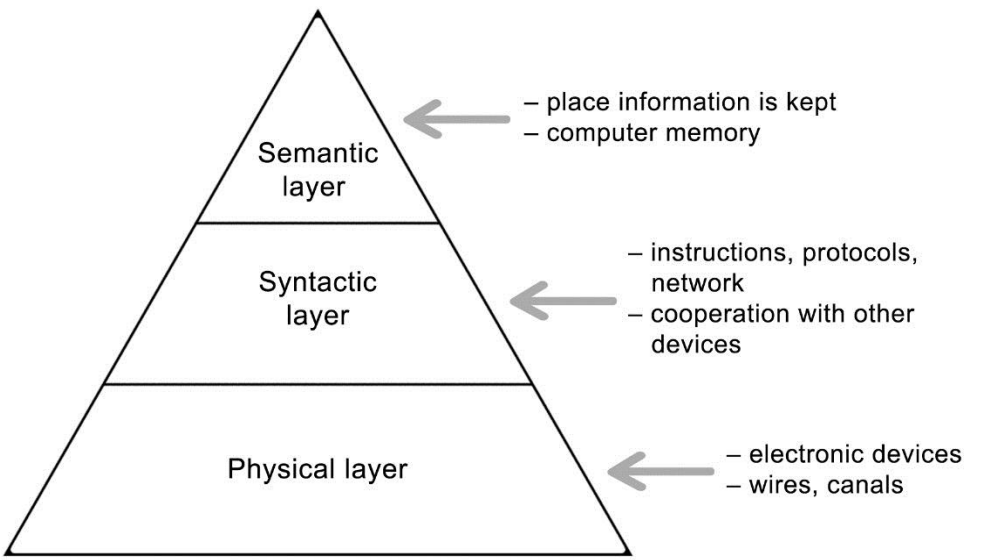
Noting the current realities of the world's processes, Professor Panarin states in his accepted theory of the fight information model chain of management that it must be completely adapted and adequate for the national telecommunication control system. In addition, it believes that effective interaction through practical operations, using appropriately selected tools, should be enriched with the experience of China and the United States[15]. To this end, he defined the management sequence, which was performed sequentially in the following steps:
– **planning and forecasting** – two parallel processes that fulfill different functions, yet constitute an effective and uniform scheme of action. Planning an information operation means a specific form of action, it refers to the elements and means used to implement a plan. Predictability is the ability to predict occurrences, in which influence and possible intervention are impossible;
– **organisation and stimulation** – organisation consists of a set of activities, based on the acquisition of the necessary resources (e.g. human, informational, financial), allowing the actual achievement of the intended objectives. In the context of the information fight, stimulation is the pursuit of information, the creation of appropriate conditions and the coordination of its flow;
– **feedback** – feedback received from the output of the output system, system or process output signals to the input signals;
– **correcting an operation** – it improves possible deviations during the information operation that may be decisive for its operation;

15 Ibid., p. 16.

– **performance check** – a theoretical concept that can be implemented as a practical activity, consisting of procedures, instructions, principles and mechanisms. Control of the implementation of the operation supports the management process, which leads to the acquisition of the desired information and the same attainment of the intended objectives.

Libicki's Information Warfare Model

Another example of the theory that comes down to the multifaceted essence of information warfare is the modern network battle model developed by Martin Libicki. It determines the cyber space as a virtual medium, much less measurable than earth, water, air space and space and even the spread spectrum of electromagnetic waves. One of the basic ways to understand cyberspace as an environment for cyberattacks is to divide it into three basic layers (Figure 2).



Source: Own work.

Fig. 2. The division of cyberspace into layers according to the Libicki's model

These layers are:

– **physical layer** – it includes all components of a given information system, including electronic devices (e.g. computers), cables, communication and telecommunication channels, etc. It is the foundation of any system, giving it a material form;
– **syntactic layer** (located above the physical layer) – this level contains instructions that designers and users pass on to the computer and protocols so that the machines interact with another recognised device in the areas of: packet, addressing, routing, document formatting, and database manipulation, This is a particular area in the context of threats from network hackers who work most often in the network;
– **semantic layer** (which is the last element in the hierarchy and located above the remaining layers) – contains information that is stored in the devices created for this device, i.e. computer memory. Some information, such as address lookup tables or printer control codes, are intended to manipulate the system; they are in semantic form (regarding information itself), but in syntactic syntax (referring to the process). Other information, such as cutting instructions or process control information, applies to automatically controlled computers[16].

Based on the assumptions it made regarding the layered construction of cyberspace, Libicki distinguished seven forms of information warfare[17]. The concept of a network war defines a conflict that triggers processes that include special protection, manipulation, degradation and failure to provide information. Taking into account the phenomena as practical operations, he defined the following schemes by making the network interaction typology:

– **Command and Control Warfare** (C2W[18]) – as a conflict that prevents efficient execution of decision–making processes at the highest levels of command and control and infiltration of information to performers of entrusted functions;
– **intelligence based war** (IBW) – a conflict involving two actions simultaneously: the protection and monitoring of their own information systems, and the efforts and commitment of resources aimed at depriving the opponent of relevant

16 M.C. Libicki, *Cyberdeterrence and cyberwar*, RAND Corporation, 2009, p. 12.
17 M.C. Libicki, *What is Information Warfare?, National Defense University, Center for Advanced Concepts and Technology*, Washington D.C., 1995, p. 1.
18 The acronym comes from English words – command and control (often referred to as – C2).

data or knowledge resources which could potentially lead to dominance on the battlefield;

- **Electronic War** (EW) – as a conflict using its own means of electromagnetic emissions to disrupt the flow of information or completely prevent any hostile activity or technical means employed by it. Among the forms of electronic warfare can be distinguished: active and passive electronic battle and electronic support;
- **psychological war** (Psychological Operations PSYOPS) – a conflict involving a system of treatments, most often of a propaganda nature, aimed at the public in order to influence it and bring about change of views on a given subject using the resources of manipulated information;
- **hacker war(s[19])** on software systems – a conflict aimed at attacking communication systems and opponents' computers by persons who possess a number of practical and informational skills in the field of computer science that can compromise security and acquire the stored resources;
- **Information Economic War** (IEW) – a conflict based primarily on the blockade of infiltration, manipulation and manipulation of its content in order to achieve planned targets on the economic aspects of the state, which can significantly destabilise its national security;
- **Cyberwar** – a conflict that involves the use of computers, network connections, and any other means of storing or distributing information in order to carry out cyberattacks on enemy systems after planning multivariable scenarios, often of a futuristic nature[20].

19 A hacker – a person of high practical computer skills, knowing many programming languages and operational systems, and good orientation in the Internet. Hackers who have very good knowledge can even influence the higher level of safety of banks and state institutions, and they also can pose a threat to them.
In colloquial language, the word hacker became a symbol of a computer burglar, who, using remote means of access, breaks into IT systems for fun or some other purpose. It is worth remembering, though, that hacking itself is not a bad thing. It is looking for new solutions, enriching skills to be the best in your field of IT. A hacker can be a criminal if s/he uses the knowledge to commit a crime., Encyclopedia of Law, http//www.gazetaprawna/encyclopedia/pawo/hasla/haker.html [accessed: 02.07.2017].

20 J. Dereń, A. Rabiak, *NATO a aspekty bezpieczeństwa w cyberprzestrzeni* [in:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, M. Górka (ed.), Difin, Warsaw, 2014, p. 211.

Conclusions

With regard to the research question put forward, it is important to acknowledge that the models of cyberspace information identified in the form of theoretical assumptions, give them the potential to be used in cyberspace to achieve their intended purpose, most often through cybercriminal acts. Therefore, the specificity of this environment can not be understood as a uniform virtual area, allowing for a specific set of actions performed in it. For this reason, it should be emphasised that the models developed and described above are not related in any way, but have only a few common features.

In synthetic terms, John Warden's decapitation theory assumes that the greatest impact on the opponent is possible with a correctly defined centre of gravity (CoG) using the characteristics of cyberspace, penetrating all the circles defined by him. Russian models of information war disseminated by Alexander Dugin include technological breakthroughs in the East (Russia) and the West (United States), as well as national and cultural values that are crucial for the further development of practical cyber–space activities. In addition, they distinguish not only the processes in society, but also the tools, i.e. any means directly affecting the given population after the orientation of the team. For this sequence to follow certain standards, a chain of management focused solely on information processes was established. Its author is prof. Igor Panarin, who develops and complements the Eurasian and Atlantic information model in his work. One of the factors that focus on the complexity of cyberspace is its division into layers according to Martinez Libicki's network battle model. This concept draws particular attention to the fact that none of these layers can exist without electronic devices.

In conclusion, it should be emphasised that the material presented in the paper should be treated as a contribution to a broader discussion with specialists from many fields. It is also part of a larger study on the evaluation of developed information technology fight–in–cyberspace models.

Bibliography

Ciborowski L., *Walka informacyjna*, Adam Marszałek, Toruń 1999.

Darczewska J., *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*, OSW, Warszawa 2014.

Dereń J., Rabiak A., *NATO a aspekty bezpieczeństwa w cyberprzestrzeni* [in:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, M. Górka (ed.), Difin, Warsaw 2014.

Dugin A., *Gieopolitikapostmoderna*, (trans.) P. Sieradzan, „Geopolityka", 1(2), 2009.

Encyclopedia of Law, http//www.gazetaprawna/encyclopedia/pawo/hasla/haker.html [accessed: 02.07.2017].

Krautz W., *Piąty wymiar walki, czyli logiczne konsekwencje modelu Wardena*, http://xportal.pl/?p=2110 [accessed: 02.07.2017].

Libicki M.C., *Cyberdeterrence and cyberwar*, RAND Corporation, 2009.

Libicki M.C., *What is Information Warfare?, National Defense University, Center for Advanced Concepts and Technology*, Washington D.C., 1995.

Orzechowski M., *Koncepcja walki informacyjnej jako element bezpieczeństwa Federacji Rosyjskiej. Wojna w Donbasie jako study case zastosowania elementów walki informacyjnej* [in:] *Polska – Rosja, Polityka bezpieczeństwa Federacji Rosyjskiej*, M. Kaszub, M. Minkin (eds), Wydawnictwo UPH, Siedlce, 2016.

Scheffs W., *Automatyzacja działań urządzeń elektronicznych w środowisku cyberprzestrzeni i walki elektronicznej*, „Journal of KONBiN", 3(19), 2011.

Sienkiewicz P., *Wizje i modele wojny informacyjnej* [in:] *Społeczeństwo informacyjne – wizja czy rzeczywistość?, Main Library of AGH University of Science and Technology*, Cracow, 2003.

Warden J., *The Enemy as System, Maxwell 1995*, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm.