INFORMATION – A KEY FACTOR OF CONTEMPORARY ARMED CONFLICT

GRZEGORZ ROSŁAN

ABSTRACT

Security issues appear in all areas of human activity. Security is discussed in the context of the functioning of public institutions, the collection and dissemination of data and information, the functioning of armed forces and many other areas of social life. Information security is a crucial element of the contemporary society. Information and accompanying processes have in recent years become key phenomena affecting planning and decision making, social behavior or the functioning of the economy and economic processes. Based on the conclusions obtained from the analysis of literature on the subject, it can be stated that information is a factor determining the effectiveness of action, while in the military aspect it determines the efficiency of the decision-making process. The above conditions constituted the main inspiration for the author, whose aim was to present information as an important factor of a success in the armed conflict.

KEYWORDS

Information, information warfare, information operations.

DOI: 10.26410/SF_1/19/7

COL (RET) NAVIG. ENG.D. GRZEGORZ ROSŁAN
roslangrzegorz@gmail.com
Rzeszów University of Technology,
Department of Management
Department of Safety Science

Information and communication technologies are the source of a new revolution. It is a revolution based on information that is an expression of human knowledge

from the Bangemann Report

Introduction

Security issues appear in all areas of human activity. Security is discussed in the context of the functioning of public institutions, the collection and dissemination of data and information, the functioning of armed forces and many other areas of social life.

Information security is a crucial element of the contemporary society. Information and accompanying processes have in recent years become key phenomena affecting planning and decision making, social behavior or the functioning of the economy and economic processes.

Based on the conclusions obtained from the analysis of literature on the subject, it can be stated that information is a factor determining the effectiveness of action, while in the military aspect it determines the efficiency of the decision-making process.

[1] Grzegorz Rosłan assistant Professor of Department of Security Science, Faculty of Management, Rzeszów University of Technology. In the years 2016-2017 the Vice-Rector for Education and Student Affairs of the Air Force Officer School in Dęblin.

The above conditions constituted the main inspiration for the author, whose aim was to present information as an important factor of a success in the armed conflict.

The realities of the modern world induce a new threat assessment both in the external and internal environment. A modern war is not only about armies, but also – and more often – about informal actions destroying the economy of the opponent (the enemy), destructively affecting financial systems, causing social unrest and political chaos[1].

In the military sphere, the information potential of military intelligence allows you to effectively plan and carry out combat tasks, and enables the exchange of information essential for the security of the state or alliance. Nowadays, the struggle for information advantage and domination is inseparable from human activity, and its essence comes down to obtaining information about the real or potential threat.

In the *Dictionary of Foreign Words and Foreign-language Phrase*s we read that *information is equated with thought objects reflecting all forms of news, communicative items, knowledge of events*[2]. In turn, J. Seidler states that *information can be called everything that is used for a more efficient selection of activities leading to a certain goal*[3]. At the same time, he states that when talking about efficiency, it is necessary to remember that having and using the right information can be used to accomplish deliberate actions better without significant increase of material resources or energy consumed[4]. On the basis of the analysis, it was assumed that the designatum of the term "information", in factual meaning, should be identified with the name of the content of the sensual perception of the stimulus, and in the functional sense – with the information process. An informational advantage is a goal that can be obtained by conducting information operations (fight for information). An informational advantage is also a means to achieve other goals, for example political, economic or military at a strategic or operational level. The fight for information is conducted with the intention of achieving success (information advantage), but it is also conducted in order to prevent the other party (the enemy) from gaining an informational advantage.

Information as an important factor in success of the fight

The fight for information takes place from the moment the first group interests are formed. It is conducted in every field, especially in the economic, political and military areas. Its goal was, is and will be to get more information than your opponent (the enemy), mislead, surprise, and thus succeed. Since the invention of gunpowder through a machine gun, tank, nuclear weapon carrier aircraft, the one has always been successful, who first used new, surprising weapons, resulting in success in combat.

Modern times are characterized by a huge increase in the importance of computers and information technology (digital). Computers controlling modern production technologies are a factor that connects almost all areas of human activity. So there was another threshold for the development of civilization of human society. The states that used the opportunities created by the IT (computer) technology more quickly dominated the future competition. The progress

[1] M. Kwiecień, (Nie)bezpieczeństwo informacyjne we współczesnym świecie, http://www.rodak-net.com/rp_art_3804_czytelnia_niebezpieczenstwo_informacyjne_kwiecien.htm, [accessed 9.05.2011].

[2] W. Kopaliński, Słownik wyrazów obcych i zwrotów obcojęzycznych, Wiedza Powszechna, Warszawa 1980, p. 429.

[3] J. Seidler, Nauka o informacji, WNT, Warszawa 1983, s. 69.

[4] G. Nowacki, Znaczenie informacji w obszarze bezpieczeństwa narodowego, [in:] Nierówności społeczne a wzrost gospodarczy, post-conference monograph, The conference: Threats in cyberspace – Security across borders (Zagrożenia w cyberprzestrzeni – Bezpieczeństwo ponad granicami), WAT 2013.

in the development and application of information technology in the military field has been of particular importance. Means of communication and computer data centers based on digital technology allow to shorten the time needed to make the decision and then the appropriate actions (action time - reaction). This is achieved by using information technology on the sensor-based path – the decision center. The sensor constitutes all sources of information about the enemy, such as: reconnaissance patrol, agent, intelligence, radar, watch station or reconnaissance satellite, while the decision center is a command post where the decision is made at a given moment.

The use of information technology also allows to shorten the internal path of information, i.e. the route that includes the functionaries at a given command post, and make this information available at any time at any command level.

In the opinion of many theoreticians studying the development of civilization, information has already become a decisive factor stimulating the process of development and progress. Information also plays a decisive role in the way armed conflict is conducted, which is not only on the battlefield but in the area of information. It takes particularly distinct shape during the transition of a given country from a lower to a higher level of development.

According to the wave theory of Toffler's civilization development[5], the world as a result of diversity of levels of development is currently at three levels of existence, i.e. agrarian, industrial and informational communities (Table 1)[6]. Highly developed countries have reached the level of the information society, the feature of which is information combining three basic factors of production, i.e. labor, capital and land.

In Toffler's opinion, the world in the first half of the 21st century is at the above-mentioned three levels of development. The transition from a lower level to a higher one causes conflicts, resulting from the conflict of interests, competition, and the desire to dominate the periphery by the more developed center over. Achieving a higher level is possible only when acquiring new production technologies, especially computer technologies, i.e. information. Thus, a close relationship is established between the progress of civilization and the information that needs to be fought for. The necessity to fight for information led to the emergence of new forms of conflicts and ways of their resolving, i.e. fighting in the area of information – Information Warfare.

Table 1

	PERIODS OF CIVILIZATION	AGRARIAN (1200-1650)	INDUSTRIAL (1650-1950)	INFORMATIVE (od 1950)
1.	structure of society	hierarchical-tribal	homogenous nation state	individual global conglomerates
2.	economy	work and trade	capital and raw materials	knowledge and symbols
3.	products	natural resources	mass production goods	information and software
4.	waging war	man against man	mass destruction	impacts with precision weapons

[5] Alvin Eugene Toffler (1928-2016) – American writer of Jewish descent, a futurologist, mainly known for his writing about the digital revolution, communication revolution, corporate revolution and technological singularity.

[6] Zob. A. Toffler, H. Toffler, Wojna i antywojna. Jak Przetrwać Na Progu XXI Wieku? Wydawnictwo Kurpisz 2006.

Fighting in the information area – a quality of a new conflict

Internet computer connections, which characterize the world at the beginning of the 21st century, caused that information is widely available. The ease of access to information generates new threats. One of the basic threats is the possibility of uncontrolled leakage of confidential and secret information. An example of the fact that this phenomenon cannot be underestimated are numerous attempts to break into government computers. The second much more dangerous threat is the emergence of the possibility of influencing individuals and organizations of states on others by sending false information, i.e. disinformation.

The significance of disinformation in the course of armed conflict was already appreciated by the philosopher and commander in ancient China Sun Tzu. He wrote: *All warfare is based on deception. Hence, when able to attack, we must seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near. Hold out baits to entice the enemy. Feign disorder, and crush him*[7].

In the contemporary conflict, therefore, the decisive role is played not only by the number of armored and mechanized compounds, the maintenance of which is very expensive, but information. At the same time, the states – to maintain competitive ability and ensure development - are forced to look for the possibility of using more and more modern information technologies.

At the same time, in the military field, information systems connecting the sensor with the decision center are increasingly dependent on modern civilian technologies, which are available only to highly developed countries. Thus, the vulnerability of less technologically advanced states to the impact of the former will increase. This vulnerability may be so large that it may even disrupt the functioning of the state's basic organs.

The resulting conflicts can be resolved without the involvement of armed forces, which as a result of the blocking of information necessary for their functioning, will become unable to operate efficiently in a given area or environment. Activities aimed at paralyzing the state's information system are nothing more than a struggle in the area of information. Such a fight involves not only the military area, but the whole society, because it will not only run between political and military opponents, but in every field of competition.

However, the notion of fighting in the area of information should not be understood as the use of only intangible means of influence, but also the physical destruction of the devices of the opponent's information system. This fight is carried out between command and control systems, involving bodies for acquiring, processing, transmitting and using information, as well as those that participate in disinformation, interfering with the reconnaissance and command systems of the enemy. So in contemporary conflicts, not the armed combat systems of the potential enemy, but his "nervous system" should be destroyed first. Actions to achieve this goal can therefore be called a struggle to gain dominance in the area of information.

[7] Sun Tzu, (544 p.n.e.-496 p.n.e.) – one of the greatest ancient thinkers of the Far East, the author of ***Martial Arts***, the world's oldest textbook of martial arts. Sun Tzu, Sun Pin, ***Sztuka wojny***, Gliwice: One Press, Helion 2008.

Forms of fighting in the area of information

Fighting in the information area, like combat operations, takes both active and passive forms. Active forms include offensive actions aimed at obtaining information and disrupting the enemy's command and control system. Passive forms of struggle in the area of information include defensive actions, i.e. protection of own information system. Both active and passive forms strive to maintain dominance in the area of information. At the same time, all undertakings are carried out to improve the effectiveness of their own information system.

The fight in the information area can be considered at the strategic and operational level. In strategic terms, the opponent (the enemy), as a coherent system, consists of the following elements: a command and control subsystem, economic resources, infrastructure, population and armed forces. In this sense, fighting against the enemy translates into separating the individual elements and destroying them. Combating the armed forces in a potential conflict will be an important success factor only at the operational level, where a precise attack, interfering with and destroying the command system of the enemy while ensuring freedom of action will enable success in the operational scale. At the strategic level, the fight for information concerns global problems and takes place in the area of geopolitics, geostrategy, as well as the economic policy of the state. In the purely military dimension, the struggle in the area of information aims to achieve the deterrent effect, and so it will be the actions that discourage the potential opponent (enemy) from undertaking aggression. On the other hand, if it is necessary to take intervention measures, it will be aimed at creating a sense of threat. The fight in the area of information at the strategic level will be organized and run by the central management of the state (coalition).

At the beginning of the 21st century, the most important security threats are: international terrorism, uncontrolled population migration, international drug trafficking, organized crime, threats posed by trade and smuggling of arms, and the threat of free transit. The second group of threats are ethnic, racial and religious conflicts of local and supra-local character, on the verge of war.

In the operational dimension, the battle in the area of information concerns an opponent (enemy) on the battlefield in relation to which a specific military operation is conducted. Besides the land, air space, space or sea, it will be performed in the digital area, i.e. in the dimension of the electromagnetic field (cyberspace). In the opinion of the author, it will be necessary to pre-empt the domination of information in order to successfully carry out air, land or sea operations in the future.

Types of fighting in the area of information

According to Western experts' views, fighting in the area of information can be divided into the following types[8]:

- Command and Control Warfare, that is, disrupting the command system;
- Intelligence Warfare, that is, counteracting to disrupt and disorganize the recognition system;
- Psychological Warfare, that is all actions aimed at disrupting the psychological immunity of the enemy's army and society;
- Electronic Warfare, that is, undertakings aimed at interfering with all electronic systems;

[8] Zob.: JP 3-13.1 – Joint Doctrine for Command and Control Warfare (C2W), JP 3-54 – Joint Doctrine for Operations Security.

– Economic Information Warfare, that is, the fight against and economic information;
– Hacker warfare, that is, activities involving hacking computer systems;
– Cyber warfare, that is, getting information from scientists and organizations, for example brainwashing.

Hacker warfare and cyber warfare differ in the purpose of aggression; the former is directed against data processing systems, the latter against people.

The course of the fight in the information area

The course of the fight in the area of information can be divided into the following stages: acquisition, electronic fight, confusion, transmission, elaboration, support of the decision-making process and protection of information. The process of obtaining information consists in gathering, segregating, pre-analyzing, drawing the first conclusions and controlling the truth. Electronic war includes the electronic recognition, incapacitation and disorganization of the work of the opponent's electronic means and systems as well as the protection of its own command and communication systems. Confusion should be understood as a series of projects related to masking, disinformation, misleading, surprise, identification, navigation and introduction of viruses to computer networks. In turn, the message includes communication maintenance, development of computer (IT) networks on the battlefield as well as multimedia and electronic correspondence.

The development of information as a next stage of struggle in the area of information includes multimedia development, merger and data integration. Support for the decision-making process consists in enabling the work of headquarters and staff in digital command systems during the development of decisions, i.e.: information analysis, location assessment, searching for alternatives, making the decision itself, planning, performing an operational plan, putting tasks (directive, order), organization operations and organization of command and control. At this stage, the important task of fighting in the area of information is electronic fire control. The last one, or information protection, includes development of modern information protection systems, secretive command, censorship, identification and navigation.

Conclusions

The evolution of the battlefield and the dynamics of phenomena determining the course of contemporary conflicts are factors that affect the shaping of the attitude of states to the issue of national and international security. These transformations have a direct impact on the way of creating and implementing national security strategies and policies.

The growing importance of the information necessitates changes in the theory of military art and views on the role of conventional combat. Therefore, the main investment objective should be directed at the development of information technology, the use of which significantly increases the rationality of decisions made and the accuracy of attacks. Thus, due to the increased expenditures on IT systems, without the need to look for new types of weapons, it is possible to significantly increase the effectiveness of those present in arming troops. So in the future battlefield, not the quantity, but the quality of the weaponry and the systems guiding it will determine the effectiveness of the operation and the potential success.

Contemporary and future conflicts are characterized by the use of more and more precise strike force and the growing role of indirect fire. The introduction of more and more modern information technologies

means that the decision-making process is getting shorter and shorter. The success of a military operation, in addition to traditional factors such as space, time and strength, has the decisive influence and information. The space also includes space and the area (environment) of information. Thus, forces due to the high precision of combat means, capable of executing strikes with indirect fire, will be smaller, more specialized and capable of immediate action. Nowadays, information in the tactical dimension has become a kind of a new kind of weapon, while in the operational dimension it is the basic factor of achieving the final success – obtaining an advantage in the area of information. In turn, in the strategic dimension, next to air, land or sea operations, we are talking about an information operation (information war) as one of the dimensions of the war.

The growing role of the information factor causes that it has become the base for air, land or sea operations, that is, it has become a key to success in a military operation. It allows you to win an operation or a war using fewer forces and resources, with fewer own losses and in less time.

Recapitulating, war as a phenomenon has been accompanying humanity since the dawn of its history. Along with the progress of civilization and the increase in the value of new, immaterial resources, there are other reasons for the conflict. At the same time, obtaining an informational advantage will require mastering the acquisition of information, its use and manipulation in order to achieve political and military goals.

Bibliography

Goban-Klas T., Sienkiewicz P., Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania, Wydawnictwo Fundacji Postępu i Telekomunikacji, Kraków 1999.

http://www.europarl.europa.eu/plenary/pl/texts-adopted.html, [access: 17.01.2018].

JP 3-13.1 – Joint Doctrine for Command and Control Warfare (C2W).

JP 3-54 – Joint Doctrine for Operations Security.

Kopaliński W., Słownik wyrazów obcych i zwrotów obcojęzycznych, Wiedza Powszechna, Warszawa 1980.

Kwiecień M., (Nie)bezpieczeństwo informacyjne we współczesnym świecie, http://www.rodak-net.com/rp_art_3804_czytelnia_niebezpieczenstwo_ informacyjne_kwiecien.htm, [access: 9.05.2011].

L. Bełza, Gra informacyjna o wpływy i dominację, Bezpieczeństwo narodowe nr I-2011/17.

Liedel K., Piasecka P., Wojna cybernetyczna – wyzwanie XXI wieku, Bezpieczeństwo narodowe nr I-2011/17.

Nowacki G., Znaczenie informacji w obszarze bezpieczeństwa narodowego, [w:] Nierówności społeczne a wzrost gospodarczy, opracowanie pokonferencyjne, Konferencja: Zagrożenia w cyberprzestrzeni – Bezpieczeństwo ponad granicami, WAT 2013.

Prońko J., Bezpieczeństwo, zagrożenia, kryzys w kontekście kierowania organizacjami, rozprawa habilitacyjna, Akademia Obrony Narodowej, Warszawa 2010.

Seidler J., Nauka o informacji, WNT, Warszawa 1983.

Sun Tzu, Sun Pin, Sztuka wojny, Gliwice: One Press, Helion 2008.

Toffler A., Toffler H., Wojna i antywojna. Jak Przetrwać Na Progu XXI Wieku? Wydawnictwo Kurpisz 2006.

GRZEGORZ ROSŁAN – Colonel (Res.) Navigator, PhD, for many years connected with the National Defense University, where he was awarded a doctoral degree in military sciences. Currently, an assistant professor at the Department of Security Sciences at the Faculty of Management at the Rzeszów University of Technology. His research interests are related to the military security, air threats, armies of other countries and reconnaissance activities.