INFORMATION IN THE AREA OF SECURITY. NEW PARADIGMS

Roman KWEĆKA

Col. (ret.) PhD, Assistant Professor, Institute of Security Systems Engineering, National Security Faculty, National Defense University, Poland

This article proposes a qualitatively new approach to concepts such as: information, area of information security, information security and information warfare. Moreover, it presents the information paradigm and information security paradigm. The diagnosis of processes and information systems of the organization in information warfare has been focused on praxeological aspect of the warfare itself, especially on its unarmed form, as the climax of a negative cooperation between the entities in their security space.

Key words: *security, information, data, paradigm, information warfare, information security.*

1. INTRODUCTION

The revolution in information technology has led to the creation of subspace in the area of security of organization (1), which dominated it completely, and the previous models of acquisition and protection of information assets have been placed under uncompromised verification. The information subspace (later: the information space) not only is a kind of 'melting pot' of the exchange of data between components of the security system of the organization, but also a reflection of their mutual relations and connections. Information resources of the organization are not a qualitatively new phenomenon in the area of security. In contrast, a completely new quality are the phenomena and processes (2) related to their generation and their availability, which results from the aforementioned revolution. So what is the nature of these phenomena and how they affect the area of security of organization?

Security of organization (3) is dependent on the efficiency of cyclical processes, including early typification of challenges (4), allowing creation of entities' ability to eliminate threats and seize the opportunities in the area of security. These processes are executed by the tools at the disposal of the organization.

At the beginning of the creation of the foundations of the modern world, space and time were a kind of shield for the flow of information - a shield that allowed as unthreatened and stable development of those who created these foundations. Next to each other grew and vanished civilizations knowing little about themselves, their desires, aspirations, and accumulated knowledge. Knowledge was the domain of cult centers and was a taboo for the uninitiated. It was easier to govern, pass judgment and provide everything. With the development of means and methods of communication, the world began to shrink rapidly. Various dimensions of good and evil were explored, acquired were new technologies and ways of using them to shape the area of security. Tribes and groups began to gather to form the foundations of modern statehood. The objectives of a single man slowly became objectives of specific societies [1].

For centuries, the world made choices of lifelong friends and enemies, connected, shared, appointed and dissolved coalitions. Ancient tribes and groups were replaced by certain subjects which today follow the same goals and objectives, which have contributed to their creation. However, thanks to the ubiquitous information processes, their territory is no longer limited only the immediate surroundings, as in the past. The influence zone can now reach hundreds of kilometers away from the state - hegemony, therefore nothing stops the realization of even the most extreme aspirations and ideas.

The problem of general access to information, devoid of political superstructure and interpretation, stands in the way of the creation of positive cooperation between the parties today, just like centuries ago.

The information policy of the governments of the era of the Cold War prevented the free exchange of ideas and experiences in the creation of global and regional security, as seen in a simplified way, through the prism of good and evil. This view for many years focused the definition of security on the prism of threats and ability of effective defense (or lack thereof). The end of the twentieth century brought the destruction of one of the hegemonic powers. In its place arose a void, there was no ‘bad’(5), only ‘good’ remained. However, this ‘good’ had and still has too many middle shades in its palette, because too many colors and substances have been mixed throughout the twentieth century. With the lack of pressure by ‘bad’, the forces between these substances and colors, within these human creations, dissolved as well. The world has become a patchwork of different aspirations and ideas, although in this ‘society of the information age’ - as defined by Tofflers, we do not notice or we try not to notice the problem.

The beginning of the twenty-first century has brought revolutionary technology development in the field of collecting, processing and use of information. Holders of information, this contemporary ‘golden fleece’, can build up and tear down any pieces of the puzzle, which our world consists of, in accordance with their intentions. In our eyes coalitions broke down and formed, as well as links and systems in the area of security of subject, which - together with technological progress and increase in the possibility of obtaining and distribution of information - undergoes rapid transformation.

Free access to information and, above all, its uncontrolled flow can consequently lead to information chaos and manipulation of information in area of security, and thus generate a negative (less positive) effects of its impact on the actors and their tools. The boundary between the neutral use of information processes for the benefit of entities, and their use for social engineering ways and methods to shape society according to the will of the political elite is very subtle and unstable.

What this may result in, the world discovered already in the era of bipolar structure. Modern hypermedia (6) have much greater strength and range of impact than their early counterparts from the sixties of the last century.

Area of global security, composed of actors and tools that these entities have, along with the information processes, necessary for their functioning, as well as phenomena independent of business entities - is the same for all states, phenomena and processes that depend on these entities. Information processes create specific relationships between entities and their instruments, they form their cooperation with each other and form its inherent characteristics. This means that information processes or derivatives of their functions are the determining factors for all states, phenomena and processes in the global security area.

2. INFORMATION IN THE AREA OF SECURITY OF SUBJECT - IMPLICATIONS

The globalized world surrounding us, and its ubiquitous "holy grail" - information, convince us daily of the need for a qualitatively new approach to the problem of security of the organization. Knowledge and findings in this area based on existing theories of information, war, peace or theories on globalization deviate too far from the real challenges of everyday life.

Today there are qualitatively new development megatrends in the area of security of entities based on the multi-faceted use of information in the fight for global domination. This phenomenon is not fully noticed by the political elites not being global HEGEMONS.

Is the above thesis correct? What arguments can confirm it or disprove? It should be noted that the utility of entities (including special services) have instruments that may be used to manipulate the information available in hypermedia in real time, infiltrate the end users and distribution of content in line with the needs of specific political elites at all available media, especially social networks. If we add to this the ability of the media to create a "live" real relationship with false events [2], we can easily see that the modern hypermedia, are a "Pandora's box", the "opening" for the use of certain players can bring events over which no one will have control in critical moments.

Changing character of security area and its "submission" in relation to information processes happening both in its core and environment, is clearly visible in the space which includes the virtual and the real world of modern man, where truth is not always true, and false ideology can become truth.

Modern capacities and hypermedia's driving force in the activities of public relations agencies and their ability in influencing the development of the structures of global security, can raise understandable concerns. They can also, as well as other above comments, confirm the thesis of a qualitatively new megatrends in security area.

The eternal processes of acquiring, holding and processing of information invariably accompany man in all cognitive processes. They become the "Achilles heel". Why? It's easy! The result of these cognitive processes is the knowledge [3] that we have, but it can be "forged" for certain entities (states, organizations, political elites, etc.). If we remain passive recipients of hypermedia "pulp" information, without a thorough knowledge of our history and the world around us – we will speed up the time when Orwellian (7) perception of the world, through the prism of the matrix (8), will be ours.

Information is the strength and power of political actors (players) who have it. In this group we can also include the world media and their owners. Indeed, like the language that we use every day, the media in their basic functions can transmit information, express or induce specific internal states, which can finally become a impetus to the implementation of certain actions or omissions.

Media administrators, using undeniable human need for reliable information, as well as the human desire to create the vision of the world around us, sometimes reach for sensational and unverified information, or deliberately manipulated. In the area of political struggle the media constitute a tasty "morsel" for any opposition, both the internal and international actors, unfavorable towards policies and strategies of the organization, power over which they are currently seeking. It should be emphasized that the information processes are a key element of the power of the organization and are not equivalent to the power of the military, economic or otherwise, they are far above them in order of importance and they determine the stable development and survival of the organization.

The rapid development and dynamic changes in the sphere of information technologies, result in a well-known saying that the world begins to "shrink" and change in the proverbial " information village." In a world dominated by hypermedia means of social communication and hypermedia systems of managing elements forming the structure of the organization and its tools, occurs a specific reduction in time and space. We intensively explore all possible spheres of life and dimensions of our world, mutually combine them together, connecting, among others, artificial intelligence with virtual reality, universe with nanotechnology, and we do everything at a rapid pace with even greater precision.

In the context of these phenomena, we can accept the thesis that information processes will dominate security area of entities in an irreversible manner and independently of the general population. Information technologies of the future and what they bring with them are therefore a challenge for the present and future political elites responsible for strategy building of information security of entities. There are a challenge that may represent both an opportunity and a threat to shaping the security of organization.

Unlimited access to information processes in modern societies brings closer the moment in which "power will come in the hands of the people." Society, having unlimited access to information, the ability to quickly share it and spread, can increasingly affect the nature of the policies and strategies implemented in the area of security. Ubiquitous media have substantial impact on the attitudes of politicians who create action of entities (their policy and strategy). They are taking activities of the organization in the international arena and in the area of domestic policy "under the microscope", exerting enormous influence on public opinion, and thus they can help or ruin many political careers. The very awareness of this fact, for many of those responsible for policy and strategy of the organization, is sufficient “brake” of their actions or, on the contrary, opens the way for demagogues and people struggling to make political capital [4]. The existence of a discussed trend can significantly affect the shape and nature of future conflicts and thus can mean an unprecedentedly strong, direct trend of impactful social factor in the area of political decisions concerning the nature and time of commiting organization's tools to action in the area of security.

In the area of communication with the public and openness in terms of information about the political aspects of the actions taken - we should expect major changes on the part of the elites in power - changes to reduce these trends.

Openness in dealing with the media threatening the loss of information vital to the security of the organization is difficult and even impossible to accept, of course, assuming that the political elite of the organization are ready for functions that they serve.

Social engineering pillars and tools of influence determine the process of informing and communicating with the public. Social engineering, which is rare between sciences, allows controlling human behavior through the manipulation and influence. Derivative associated with the impact of social engineering tools is the ability to create facts, using tendencies in societies for cheap sensationalism in search of alleged hidden motivation, helping themselves with a conspiracy theory and modern techniques of virtual reality. These actions may not only lead to the collapse of morale, but also can erode the value system and influence the behavior of societies [5]. Information processes are a qualitatively new, not fully noticed by decision makers, environment of the future war. The problem of war "with" and "for information" will increasingly absorb the operations of the organization and its tools in the area of security.

Information is in essence an elementary factor in all organized activities. Without information on the current situation of decision-making it is difficult to take steps, which will provide a guarantee of achieving the intended objective. In other words, every purposeful action requires information, which bring the active organization border, which that organization seeks. This thesis does not refer only to the area of information war or generally armed struggle. The assessment of each decisive situation, that is taking action with specific purpose, after all, it is the domain of our everyday life in all its manifestations.

What then is the very information that is so important for any intentional actions? This is the basic concept, difficult to define using simpler concepts. S. Koziej defines information as "intangible factor aggregating other factors of armed struggle in a harmonized whole armed conflict". L. Ciborowski defines information as "stimulus" (9) affecting man's reception system, causing creation of the object of thought in his imagination, reflecting the image of things material or abstract, [...], which in his opinion (consciousness) is associated somehow with this stimulus. [...] Its existence is relatively connected with the existence of man and his mind [6]" J. Seidler defines information as "all that is utilized to a more efficient selection of activities leading to the realization of a particular purpose," thus emphasizes trade of information with intentional actions. Father of cybernetics N. Wiener defines information "as the name of content taken from the outside world, as we adapt our senses to it," assuming that "the process of obtaining and using information is the process of our adaptation to various contingencies of external environment and our active living in this environment. "

It should be noted that in information theory emphasizes that the information is all that is neither energy nor mass. Can we uncritically accept this point of view? Is information really neither energy nor mass?

Man has a limited perception of most of the available signals in nature and artificially generated electromagnetic spectrum, which needs specific "sensors" to allow free access to information.

Indirectly aspect of "adaptation of the senses" can be found in Wiener's determining of the information. The fact that we just do not have a "transmitter" of signal does not mean that there is no information currently available to the world. It is only our limited perception that deprived us of the possibility of direct reception, which is a carrier of information. This seemingly obvious fact is often overlooked in the discussion about the nature of the information.

We define information customizing each of its definition to the current needs, refuse it having energy and matter, but while speaking of information we are in fact talking about carrying the signal. With its energy, mass and characteristics shaping the signal. If we agree with this reasoning, the consequence of this would be a statement of fact that information may also exist without the human mind. However, it cannot exist without carrying signal - which means that the information is essentially a form of matter, along with the specific energy for this matter.

In the information processes we deal with signals, which are the carriers of information, or a certain form of matter (10) and energy (11).

In reality around us we do not have access to the information in its "pure" original form. We have access to the data, which are a form of mapping signal carrying information. In the theory of information, the data used to be called potential information [7]. In the language of description, the data is as if in a "hibernation" information which is "excited to live" in a specific decision situation. In other words, the system receives outside information, and according to its content responds to an apparent state of affairs, or process. How, then, to define the information to meet all the conditions outlined above? Assume, therefore, that:

"Information is a specific portion of the energy accumulated in the material mapping [8]" - the basis for creation of information in general, is the existence of the signal carrying it, materialized in the form and shapes possible to process and interpret it by man. Accordingly any information protection from the point of view of existing solutions (information and technology) and the possibility of access to the signal carrying it is a much complicated matter - if not impossible.

Cognitive abilities and the desire of man to acquire specific knowledge are sufficient driving force to allow for breaking all barriers, even the methods commonly considered to be unlawful, on the way to taking over sensitive information to other entities. The road, on which information must "travel" from its creator to recipient (the organization or entities for which the benefit has been produced), is its ability to protect against "hostile takeover." These abilities do not stem only from the technical conditions or technological means of communication, but depend largely on the organization to which the information is addressed. The final recipient of the information and its further "distributor" is usually the man who, knowing the strength and the causative abilities of information processes may use it contrary to the assumptions of its creator, regardless of the danger threatening him - including legal repercussions. A typical example is the so-called "Snowden affair" [9] (Edward J. Snowden, a former employee of the CIA and NSA, wanted on charges of disclosing state secrets and espionage for providing information on PRISM to the press - footnote RK).

3. INFORMATION PROCESSES IN THE AREA OF ORGANIZATION SECURITY

Elements of the structure of the security are so interrelated that a change in any of them entails changes in the other components. These changes synergistically influence the course of the processes taking place in security area. Elements of the entrance and exit "encoded" in the security area are generally consistent with the "input and output" elements of all subspaces, which affects the security process. This process is generally an unstable process characteristic for any artificial system. Its environment is the set of all subspaces which do not belong to the security of the organization and which properties affect it and also change under the influence of its (organization's) actions. It is obvious that the security area of organization defined as artificial framework of its security system must interact with all systems functioning in its environment.

Recognizing the priority role of information in a deliberate action, we should also identify it with the informational processes of organization's security area. How, then, information processes are implemented in organization's security area? How do these processes affect the evolution of the decisive situation? How to locate information processes in the area of security of organization?

Surrounding area of security stimulates information processes external to the control systems (decision-making) (12) and interaction objects (13), meaning it directly affects the power processes. This means, among others, the fact of direct impact on the signal carrying the information in the internal information processes. Thus, it is possible to input disturbance in the operation of these processes. This is obviously an aspect of information war (warfare) (14). The interior of security area in the information processes is described by the processes controlling shaping of information security policies and strategies of the organization, information processes and internal control systems (decision-making). Reverse information processes provide specific feedback loop of control system with a temporary state of affair or process. In each of these processes, we can identify a specific type (15) of information, reflecting the correct phase for the cycle stage of organizational activities. Let us mention therefore three basic types of information: external information - manifested in the control function of the decision-making system or the impact function of the environment on the object of interaction; inside information - reflecting the state of knowledge of the decision-making system about impact objects or external conditions (system environment - note the fact that the object of the impact of the control system are all objects that can be found in the impact area; this applies both to own tools of the organization, as well as a potential ally or the opponent and the facilities included in the information systems) and feedback - as a reaction of impact objects or effects of the decision on the external information. Feedback is essentially a reflection of the information processes carried out by specialized tools of organization (for example special services). It means the relationships between systems of decision-making and interaction of objects (including perceptual systems) in the information processes taking place in the area of security. In other words, they are the feedback between the decision-making system and all the tools of the organization. Discrepancies fixed in relation to feedback allow management processes informational organization, thus allow achieving a higher degree of determination in the creation of the area of security.

Dual interpretation of information processes (in the light of the principles of information theory and activities organized), allows you to define their essence in the process of creating a security of organization. It also enables the formulation of specific features that modern information war (warfare) imposes on information processes. Without taking into account these characteristics it is impossible to "design" the appropriate power process in this area. In light of the aforementioned theory, we can distinguish at least eight such specific features. These are undoubtedly creativity, interdependence, autonomy, integrity, availability, flexibility, regularity, and punctuality (16) and they are to be understood as follows:

- Creativity - information processes represent both cause and effect of power processes.
- Interdependence - information processes and power processes are inextricably linked.
- Autonomy - each subsystem of information war (warfare) should have its own, independent subsystems fulfilling the functions of systems of perception. The data obtained through them should fully protect the needs of the rational use of subordinated instruments of influence.
- Integrity - any information processes performed by the subsystems of the information war (warfare), are an important complement to studies and analyzes conducted by specialized structures of tools of organization. This means that the data from stand-alone information systems should be strictly transmitted for study activities of specialized structures of tools of organization.

- Availability - due to the nature of information processes, and particularly the need to ensure the security systems of perception, collection, preparation and distribution of the acquired information is provided by specialized tools of organization. However, the difference between the need to preserve the security of the data and blocking it on the wrong levels of decision-making (or tools) should be definitely distinguished. The data should be available on any request of an authorized decision maker, without revealing their source, but with a specific clause stating degree of reliability and validity.
- Flexibility - permanent order, formalized and established procedures in the processes of information increases their efficiency. System of operation and procedure, however, cannot limit the imagination and initiative of subordinate subsystems. Information processes have to meet unexpected changes in the area of information war (warfare), so the information must be capable of immediate response to this decisive situation in the area of security.
- Regularity - in information processes it is necessary to analyze the data, distribute information and it is necessary to manage systems of perception of tools of organization. The continuity of these processes determines achievement of advance information, thereby avoiding surprise with a potential crisis in the area of security of organization.

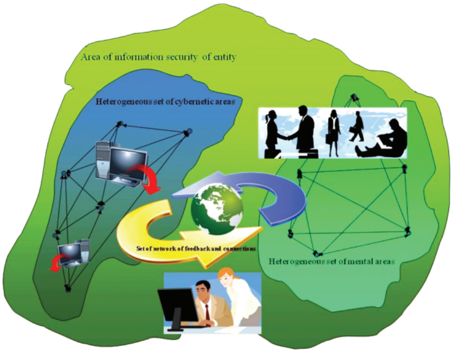
Area of information security of entity
Heterogeneous set of cybernetic areas
Set of network of feedback and connections
Heterogeneous set of mental areas

Fig. no. 1. Information processes in the area of security of organization
Source: R. Kwećka

Creating an overall strategy of activities of the organization is performed in an area dominated by time and information, because regardless of changing governance and political order in the area of security of entities, these two factors are still spiritus movens of all organized activities. Force, once necessary in the struggle for hegemony, was replaced by a synergy in the activities, and the need to take over the area of the opponent - the precision impact on it and its entourage. Precision based on accuracy, clarity and exactness in creating the rules of the political game and strategy of entities in relation to the interaction of objects.

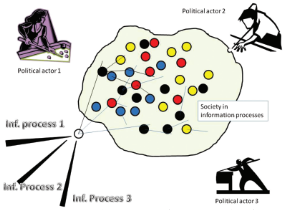

Fig. no. 2. Transformation of determinants of changes in creating the strategy of entities
Source: R. Kwećka

4. INFORMATION SECURITY OF THE ORGANIZATION

Specified complexity of the structures forming the organization (the state), the number of its component elements and a multitude of internal and external relationships, create a situation where the researcher is able to create only general regularities that govern its development. Dynamic changes in the security of the state, including in the area which belongs to its environment may lead to the thesis that only intellectual and conceptual preparation might allow reducing risks,minimizingtheconsequences of their occurrence and the skilful use of the opportunities that arise, and thus meeting the challenges of the future [10].

Ubiquitous media have a substantial impact on the attitude of the political elite in power, which create actions of entities. They are realizing their own objectives (audience, profit, informing the public), and they take activities of the organization in the international arena and in the area of domestic policy "under a magnifying glass". They have enormous influence on public opinion, both in the internal and external aspects of organization (state). Particularly noteworthy is the strategy of national security that determines its activities in the area of information security. Information is an essential, if not decisive about everything, determinant in shaping policy and strategy of organization. If we attempt to grasp hierarchical determinants in terms of their importance to the security environment, no doubt the information would be on top of this kind of “top list”in relations between the entities. Let us note that the above findings clearly indicate the dominant role of information in the process of creating a security strategy of organization.

Information security strategy is a kind of polystrategy of security of organization. It is present in all sectoral strategies, plays a dominant role in their creation and protects the vital interests of the organization, while providing the key to the creation of superiority and information domination of subject in the area of security (17).

If, in the steps of Józef Kukułka, we accept the rules of the evolution of the concept of strategy, generated by it, along with the reasons accompanying them, the above observation is fully justified, because as prof. Kukułka writes: "the way from the classic military strategy to polystrategy means the process of withdrawing its monopoly from a narrow group of specialists and bringing it to the various groups of professionals. Thanks to this, the rank of polystrategy seriously increases because its formal and substantive relationships with the general policy of the state are much closer than the compounds of classic strategy [11]" The words on the "narrow group of specialists" can be applied not only to military strategists, but also to the representatives of the so-called group of IT specialists (Information Technology) (18).

Information security goes far beyond information technology, it is present in every manifestation of the organization, deciding on its capacity for sustainable development and survival.

In the available literature, the security information is usually identified with security in cyberspace, information technology area or telecommunications infrastructure of the organization. In the vast majority of studies, especially in the US, we find references to cyberspace (19) understood as a specific physical domain, which is "[...] the result of the creation of information systems and networks that allow interactions electronically. [12] " In a similar manner information security is defined through the lens of the computer area or telecommunications infrastructure, thus narrowing the area of the security only to the structure and level of security existing in the area of information technology. Such an approach to the problem causes significant "blur" to the essence of information security, which usually manifests itself as the lack of a common (combined) strategies, the effect of such an approach are uncoordinated activities of the organization in the field of security, usually carried out based on the guidelines and principles in different sectoral strategies.

Implementation of the information security strategy is in fact a manifestation of the implementation a strategy of information warfare by the organization. A war that does not need to be officially "declared" to another organization.

A war that takes place in the mental (20) and virtual space (21), and the objects of its massive attack are (or will be) not only tools at the disposal of the organization or its critical infrastructure, but also the decision-makers and their political supporters, which may be up to new heights of power or deprived of it at any time, assuming that this may not necessarily be realized in a democratic way. It is therefore not possible to create a stable area of information security of organization without understanding the nature and significance of the issues of national security and the security area by the political elite, as well as decision-makers of all institutionalized forms of social activities, both from the public and private sectors. To this group we also need to include decision-makers of the tools at its disposal, or what an organization could have in the implementation of the strategy of national security. If we enlarge the above group with the remaining part of the society, along with the proper understanding of security and its space, we get a specific set of mental spaces. The network of connections and internal links in the mental areas and a network of connections with a group belonging to their cyberspaces, is kind of the first and the biggest area of risk for the stability and durability of the information security of organization.

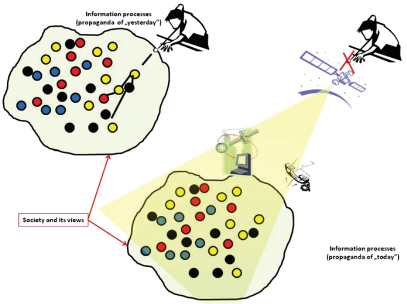

Fig. no. 3. The area of information security
Source: R. Kwećka

As a result of the abovementioned conclusions, we can state that the area of information security of organization, is the sum of three disparate sets, meaning a set of cyberspaces, a collection of the mental spaces of the organization and between them (**Figure 3**). Assuming that the "C" means a collection of the cybernetic spaces, "M" - a collection of mental spaces, "S" - a network of connections and internal links between the C and M sets, and assuming that the common element of those sets is marked by "x" and it is information - the above definition of the information security of organization can be written in the following way:

$$C \cup M \cup S = \{x : x \in C \vee x \in M \vee x \in S \ \}$$

$$C = \{x_1, x_2 ......, x_n\};\ M = \{x_1, x_2 ......, x_n\};\ S = \{x_1, x_2 ......, x_n\}$$

Let us note that the "x" (the information in its original form) is a specific form of the signal in both the mental and virtual space, as well as in a network of connections and internal links, thus it (information) plays special role in activities of the organization. It constitutes a specific response to external or internal stimulus that causes the generation process, reflecting the image or the state of affairs of material or abstract object (phenomenon, concept, etc.), which is associated directly with the adopted stimulus. Said reaction to a stimulus refers to both human (22) (mental space) as well as systems and computer models (virtual space).

The combination of two spaces, distinct in nature, along with cyberspace, placed above the virtual space, and network of connections and internal links relevant for them, creates the right area of information security of the organization.

With this in mind, we can formulate a qualitatively new definition of the information security of organization. Therefore, let us assume, that: security information of organization is the process (or momentary state), implemented (held) in of mutual positive cooperation, led by the tools at the disposal of the organization and for activities in the area of information security. These activities are carried out in an integrated National Security System of organization.

Information security is manifested in actions and processes ensuring: the integrity of information resources of the organization; effectiveness in obtaining them; purposeful implementation of actions aimed at propaganda and social engineering to produce the desired attitudes and social behavior in a real or potential risks arising from the information processes that do not have a source in the classic war.

Therefore, the above definition does not refer to the classical definitions of security and security sector of organization - absence of risk, but clearly refers to its constant presence and absence of the possibility of eliminating it. Information Security is therefore an important subsystem of the National Security System, it includes certain structures and tools of the organization, outlines its general ability necessary for stable growth and survival in the conditions of use of the opportunities and minimize the threats.

Information processes, not being a classical form of war, are the sources of threats as destructive, if not of much more character and importance to the subject, than the armed struggle.

5. THE PARADIGM OF INFORMATION AND INFORMATION SECURITY

The paradigm of information security, just like other paradigms in science, will always remain incomplete set of definitions, theorems and axioms, forming theory constituting an area of knowledge. At the same time in the course of assimilation of qualitatively new knowledge paradigm, it is constantly subject to be changed. We can therefore say that we are able to generate only certain abstracted paradigms of information security of organization, which will be an expression of the specific characteristics associated with it, rather than the paradigm as such, describing the security information in a holistic manner. It is also consistent with the approach to the essence of creating paradigm presented by T. Khun, who connected it with specific scientific achievements in the world of science and not to the notion of universal rights and points of view [13]. Referring to the security paradigm J. Gryz indicates the attributes of knowledge, defining and describing the man as the basis of its creation over the centuries. It is assumed that the basis for security paradigm of the organization are: communication, ideas, tools, aimed at ensuring the existence, development and satisfying desires, as well as feelings and passions [14]. Let us note that these four elements, interconnected and complementing one another, not only form the basis of knowledge and the theory of knowledge while they have a utilitarian use in the context of the creation of the security of organization or the creation of processes aiming at its future desired states but they also have one elementary thing in common, which is INFORMATION.

COMMUNICATION is not possible without information, any, even the best IDEA will not survive the test of time, if it is not propagated and perpetuated in society with the information about it available in the mass media. Is it possible to WANT something even without a priori knowledge (information) about desired object? The PASSIONS and AFFECTIONS are an external manifestation of the environment, is to inform about goals and intentions, this is kind of feedback in building their own "I" and individual security of organization.

According to J. Gryz "security paradigm - containing in itself the subject of security, the matter of security, the environment in which security is provided or implemented as well as interactions between these - refers to three domains that while overlapping and penetrating are creating context of knowledge and the concept of that knowledge. The first domain is the man and the surrounding world - the world of human activities, its products in the natural world of their mutual overlapping. Second, the environment in which he resides - social as well as natural. Third, the world of ideas by which the man recognizes the reality around him (ideas and ideologies build on their canvas can be distinguished due to their specific features and characteristics that define human activities, communities, societies, nations). [15] "

In both the views of K. Darwin and K. Mannheim, which J. Gryz refers to, the strong influence of information processes and creative role of information in regard to the nature of the organization's security paradigm can be found. In line with the views of K. Mannheim, those three domains penetrating each other create a context in which the organization identifies its place. Let us note that each of the domains depends on the knowledge which subject currently possesses. Knowledge is the derivative of information. Man (original organization) and his creations are a direct manifestation of knowledge based on internal information, which he possesses. Social and natural environment generate external information processes that provide knowledge of other entities (their goals, aspirations - feelings by K. Darwin), which is the basis for the expansion of their "own" knowledge of the original organization, and the search for solutions that will allow it to develop in stable way and survive in the world of ideas (ideology), which define the objectives and aspirations of others.

It can therefore be concluded that the elementary determinants shaping our perceptions of security and its paradigms are certain states of knowledge (awareness) of the organization (either a single person or entire communities and organizations created by man - the original organization). As emphasized by B. Czarnecki and W. Siemieński, prevailing in this area are psychological aspects and their relationship to the material factors [16]. Let us note that this fact may constitute a strong impact of propaganda in the information warfare (war) where we can take advantage of unrestricted range of methods, means and ways of acting on the mind and emotions of the original entities. During the Cold War, the essential concepts defining the paradigm of security was a threat, fear, and preventing them in the international forum. Dynamic changes in the international environment changed approach to security issues, as well as the peculiar evolution of the paradigm. At the end of the twentieth century, understanding security from the position of paradigm focused on the state as the central organization in a hostile international environment, gave way to a positive and constructive vision, referring to international cooperation as the basis for its development. According to J. Świniarski and W. Chojnacki "new security paradigm should in fact allow an understanding of the complexity of the modern world and reflect the real and actual changes in the international environment. An important element of the emerging new security paradigm is stressing the need for international cooperation in the process of providing it. [17]" This change in approach to security paradigm is only seemingly "revolutionary". Its essence is continuously based on communication, ideas, desires, feelings, and three domains, which are a kind of reflection in international relations, where the original organization (person) is replaced by organizations of all kinds. It should be remembered that state in accordance with the views of L. Krzyżanowski is a special organization, governed by the laws, which are subject to other “organized actions” created by man.

Scientific research on information, its essence and paradigm has been ongoing for decades. Although some interesting research approaches were created (represented by: Claude Schannon, Warren Weaver, Fred Dretske, Mieczysław Lubański), there is still no general theory of information. Information is in fact a problem for researchers already at the time of selection of methodological approach to research. It is considered, that the information processes and phenomena are too complex and varied so it has become impossible to describe them in unified way. Is this a correct thesis? With the current state of knowledge, certainly yes, but in the future, the answer will also be positive?

In 2008, Elsevier BV publishing house released the eighth volume of textbook series, "The Philosophy of Science" edited by Pieter Adriaans and Johan van Benthem entitled "Philosophy of Information". The manual is one of the most comprehensive studies of scientific disciplines, in which information plays a crucial role. At the same time it was an attempt to summarize the achievements of science in the field of information theory in general, which was successfully carried out by both authors. P. Adriaans and J. van Benthem state, inter alia, that we can now talk about three main paradigms of information. These are the paradigms of logical-cognitive, probabilistic and algorithmic. As the authors say this is due to the existence of three basic types of information, which they describe as the information as A, B, C:

Information A - Knowledge, logic, what is conveyed in informative answers;

Information B - probabilistic, information-theoretic, measured quantitatively;

Information C - Algorithmic, code compression, measured quantitatively [18].

P. Adriaans and J. van Benthem claim that presented types of information, together with the corresponding paradigms, complement each other. It comes from the fact that, although the first logical-cognitive approach (information type A) is relatively loosely associated with theprobabilisticapproach(information B) or algorithmic (information C), the other two, established mainly by C. Shannon (B) and A. Kolmogorov (C) are essentially similar. They also found that, after analysis of existing theories, they can attempt to formulate a general theory of information, although in some of its aspects lacking "something" else.

In the theories analyzed by P. Adriaans and J. van Benthem the essence of information was "blurred" in the diversity of approach, although traces of its "connection" with the wider information technology and its tools can clearly be seen, as well as a from a purely mathematical models and statistical understanding. An obstacleistoobriefandtoocolloquial understanding of information as to communicate to someone - something with the transmission of specific signals, while rejecting the fact, that information cannot exist without the signal carrying it (!). Mieczysław Lubański omits this also, although he underlines that "today we are only in the era of information technology, rather than the information itself. We process, strictly speaking, signals that - as we say - carry information. [19] "

The result of dogmas encoded in the minds of researchers is the fact that each time information is being tailored and defined according to the canons of the methodology adopted and although the researchers point out the necessity of the existence of the signal to talk about information in general, it is refused its energy and matter. Wiener also emphasized that the information is as fundamental as energy and matter, but at the same time claimed that it cannot be defined by the fundamental concepts (!)

Meanwhile, as already signaled earlier, in the information processes we deal with signals which are the carriers of information, or a certain form of matter and energy. In reality around us, we only have access to the data, which is a form of mapping (matter) of signal (energy) carrying information.

To emphasize the essence and importance of this statement, we can discuss a topic of information through the prism of "black holes" (23). For years it was thought that they contribute to the total "destruction" of given information. Meanwhile, according to quantum mechanics, information cannot "die"! This information paradox, well known to physicists for years, demolished the principle of unity of foundations of quantum mechanics. Stephen Hawking, who in the early seventies discovered that black holes may disappear along with absorbed information, in February 2014 published work [20], in which he “says that around the black hole there is no absolute horizon, and therefore never forms a closed area outside of which nothing can escape." No event horizon means that there are no black holes - in the sense that light cannot escape from them," - writes Hawking. In short, in his opinion there are no such black holes, which a hitherto unheard of - objects that they do not let anything from the inside. No event horizon means that there are no black holes - in the sense that no light can escape them - writes Hawking. For a limited time there is only "apparent" horizon that [...] allows information to get out of the depths of the black hole - information about its victims. It can be imagined as earthly horizon, which is the border, where the sky descends to Earth - on the surface it seems that you can walk to it, but it does not really exist. So there is no paradox - the information is not lost without a trace, escapes, before the black hole has time to evaporate completely [21]".

It is not important at the moment that it implies a serious distortion of information and causes trouble in reading the original content of the "mapping", the important thing is that the man who years ago contributed to the "creation" of paradox of information, as of today, using the development of knowledge (including the achievements of Polish scientists) could make significant changes in the theory, which he created, admitting thereby to an important error. In conclusion, proving "not directly" and basing on the assumptions and theories which are only indirectly "recognize" the thesis that the information is in its original essence, a specific signal form and is as fundamental as matter and energy, we can validate the definition of information adopted in earlier considerations.

Information is specified portion of the energy accumulated in its material mapping. Speaking in description language, the energy and its changes are a scalar physical quantity characterizing the state of the information, which is the real object that exists objectively, independently of the knowledge, perceived also sensually (matter). In the same time information, just as matter, is characterized by the extent of the time-space, movement and changing character, taking a variety of forms, including even extreme distortion of the content "reflecting" information while passing through the "apparent" event horizon of a black hole.

It leads to the "duality" of information as its immanent feature, which can be found in two basic processes occurring in any activity organized, and in any system, including artificial systems. Power processes and information processes are subject to permanent transformation (24), which is possible thanks to "duality" of information.

In information processes, in praxeological terms, "information" is a factor which puts subject closer to one of the expected final states, in cognitive terms it is required for the organization to change its state of knowledge (in the deliberations of P. Adriaans and J. van Benthem we can assign these attributes to “A” type information – own footnote). In the power process, seen through the prism of praxiology, as effective action, "information" belongs to the set of streams describing the information processes, in cognitive terms it is necessary for the organization to make the subject of its typification (in considerations of P. Adriaans and J. van Benthem we can assign these features to information "B" and "C", because each of them addresses the problem of "measurability" of information, they differ only in approach to the methods and scale of "measuring" - author's footnote).

In conclusion, we can assume that on the basis of the above considerations, supported by existing research in the field of information theory, conducted over the years 1994-2014 by the author (R.K.) - proposed by P. Adriaans and J. van Benthem, three basic types of information: A; B; C, can be reduced to one type - "information Σ" (Sigma - symbolic designation of "duality" of information "A" + / "B" ^ "C" /). While the three main research approaches (paradigms) to just two: logical-cognitive and an approach based on quantitative measures.

General analysis of the paradigms of security and information, carried out, allowed, as already expected, to try to generate a paradigm of information security of organization. Common features, spaces and processes that can be isolated in the security system of the organization and the information processes, which are its inherent feature, bring us closer to the object of our search. At the same time, it should be realized that the proposed solution is adequate to the current state of knowledge and in the course of assimilation of qualitatively new knowledge it will be subject to ongoing review and changes that may accompany this verification. At the moment only specific, abstracted features of security information of organization can be generated, rather than the paradigm as such, describing the security information in a holistic manner. Although the paradigm of information security to some extent remains only unfinished set of definitions, forming theory constituting an area of knowledge, it should be asessed that it will seriously contribute to the construction of information security of the organization.

The organization and the space that surrounds it, its aspirations and ideas, enriched with information processes, both "internal" (ideas), external (communication) and feedback (showing desires and feelings) - are essential features of the paradigm of information security of organization.

Organization, regardless of its degree of complexity and security space in which it operates or intends to operate, is heavily dependent on information processes. This "addiction" is a direct result of the "duality" of information, which is a component of both information processes and power processes, which has already been presented.

In the communication, ideas or desires - logical and cognitive paradigm of information reflects the form of "information". The paradigm of quantitative measures is a reflection of the "driving force" and the ability to influence the mental processes (for example change of views and ideas), or ability to act in destructive cyber systems. "Duality" (Σ) of information is an essential paradigm of information security of organization. It is the cause of any changes in the security of the organization, it constitutes an inherent feature of information, including the ability to transform power processes (another phase transformation of a particular matter and energy being or likely to be available to the organization, the desired effects of the policy and strategy) and information processes (mapping any changes that occur in the area of security) of the organization.

The paradigm of information security - containing INFORMATION "Σ" - refers to three domains, which are mutually connected and they create a context of cognition and the concept of the knowing its essence.

The first domain is the external information process - manifested in the control function of the decision-making system of the organization, or as a function of the impact of the environment on the object of influence.

The second domain is the internal information process - reflecting the state of knowledge of the decision-making system about objects of influence or external conditions (the environment).

The third domain is the feedback information process - as a reaction of influencing objects or decision-making system on the external informations. Feedback is essentially a reflection of the information processes carried out by specialized tools of organization (for example special services), which means the relationship of decision-making systems and objects ofinfluence (including perceptual systems) in the information processes taking place in the area of security (it is feedback from the decision-making system and all the tools of the organization).

6. INFORMATION WAR - FUTURE WAR

Laying the foundations of modern information warfare of the organization, one should seek specific factors that affect its present and future dimensions. The search for these determinants is one of the most important and also the most difficult tasks. Simple, intuitive definition of information warfare as the struggle "with" and "for information", results in the search for the determinants of changes in the process of acquiring (obtaining) information and processes to protect own information resources of entities.

In terms of organized activities we pursue the search for determinants in terms of positive or negative mutual cooperation, with all the consequences of these categories. We also conduct exploration in the area of offensive and defensive aspects of information warfare. However, in the offensive (defensive) activities, from the point of view of praxeology, we have to deal with both the positive and negative cooperation (warfare) if we pursue cooperation (positive cooperation) between entities belonging to the same or another area of security. We can state this kind of aspects of the impact within the country where the activities, for example defensive, processes of positive cooperation happen among its tools of influence, while the characteristics of negative cooperation (warfare) may also be found in the inner space of the state in the processes concentrated of exploration and combat of hostile agents (intelligence). A similar scenario can be seen in information activities and acquiring knowledge by competing companies (industrial and other), hence bringing all the structures and organizations to identify one - in this case - organization appears to be the benefit of this research.

Specific tools of entities or entities themselves deal with organizing all the information processes hence further determinants in shaping the information security activities are specific actors (players) implementing the strategy (policy) of the organization. Categorizing the notion of actors in the processes of information, we can make initial division into negative and positive actors (players), or actors representing the two currents of mutual cooperation, taking praxeology as a basis for categorizing. Starting from basics of categorization related to the acquisition and protection of information, we can make a distinction between offensive and defensive actors (players) or representing the two streams of information. The actors (players) coordinating and executing the tasks associated with the acquisition or protection of information for certain decision-making processes do not work in a "vacuum", the purpose of their interactions are defined information resources which are "owned" by entities. These resources can also be categorized using different basis of this categorization. The most important fact and at the same time the basis for categorization of information resources is the area of human's information resources (his mental information), which is often forgotten when considering the issue of information war (warfare) and the difficulties are seen only in the area of artificially generated cyberspace. The adjective "artificial" was used here deliberately, because it must be assumed that a person in itself creates a kind of cybernetic space, possessing millions of network connections and relationships, their own information resources and the ability to create activities based on these resources.

For the actors (players) in the processes of information, each piece of information has a specific measurable value. We can estimate its value in terms of, for example, monetary exchange or in terms of organized action manifested in bringing (actor) player closer to the ongoing organized activities. Each time the value of information will be unique and estimated, resulting solely from the fact, how much certain actor (player) will be willing or able to pay for the information resource of organization, with payment not only refering to financial issues, since it can be as well in the form of another information resource or even specific package of information, if the actor (the player) will obtain crucial information for its actions in this way (this type of situation occurs frequently when exchanging of intelligence is carried out by the special services - tools of entities).

Primary determinants of changes in the information war, forming the subject area of information security, are:

- actors (players), creating information processes of organization;
- its information assets;
- offensive and defensive information processes.

Secondary determinants are factors dependent on changes happening in primary determinants.

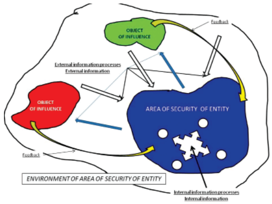
OBJECT OF INFLUENCE
Feedback
External information processes
External information
OBJECT OF INFLUENCE
AREA OF SECURITY OF ENTITY
Feedback
ENVIRONMENT OF AREA OF SECURITY OF ENTITY
Internal information processes
Internal information

Fig. no. 4. Determinants of changes in the information war
Source: R. Kwećka

Information processes in the area of security, their nature and the interdependence of processes, confirm that information processes are a qualitatively new, not fully noticed by decision makers, environment of the future war. From the point of view of praxeology, information processes are organized action, focused on the positive or negative mutual cooperation, which is a manifestation of the information war (warfare).

Modern websites are beginning to increasingly resemble a battlefield, which is fought in a completely different dimension than the one known to us from the classic war or armed struggle (although there is information is its immanent manifestation). Its essence can be seen in the struggle for information superiority and dominance. However, in this case the word dominance, it is manifested in efficiency and dynamics in reaching certain political formations, social groups and the ability to manipulate their moods and creating behaviors consistent with the needs of political actors (players). Graphically, we can illustrate this party snooker, being played in virtual and real space by the actors (players) who, through information processes, precisely target a specific environment, are able to polarize the public organization and manage it according to specific needs.

The process of informing and communicating with the public is determined by social engineering pillars and tools of influence. Social engineering, allows to control human behavior by manipulating or influencing. Derivative of tools of influence, associated with social engineering, is the ability to create facts, use of tendencies in societies to sensationalism in search of alleged hidden motivation (see the tabloids), help of conspiracy theory and modern techniques of virtual reality. Therefore, not only these activities can lead to the collapse of morale, but also can erode the value system and influence the behavior of societies [22].

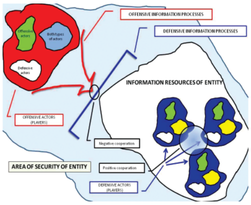
OFFENSIVE INFORMATION PROCESSES
DEFENSIVE INFORMATION PROCESSES
Offensive actors
Both types of actors
Defensive actors
INFORMATION RESOURCES OF ENTITY
OFFENSIVE ACTORS (PLAYERS)
Negative cooperation
AREA OF SECURITY OF ENTITY
Positive cooperation
DEFENSIVE ACTORS (PLAYERS)

Fig. no. 5. The struggle of political actors (players) for the information advantage and dominance implemented in relation to the specific political formation of social groups
Source: R. Kwećka

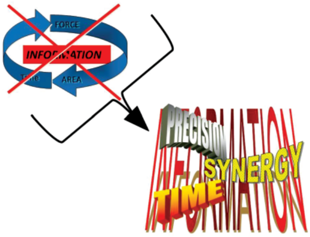

Fig. no. 6. Information warfare of political actors (players) "yesterday" and "today"
Source: R. Kwećka

In conclusion, we can assume that the thesis defining information processes as qualitatively new, ABSOLUTELY virtually "invisible" to THE "WEAK (25)" DECISION MAKERS AND USED (NOW) BY HEGEMONS, environment of the future war - is completely legitimate.

Activities and processes, which constitute information warfare, are carried out under conditions of actual or potential risks arising from the information processes that do not have a source in the classic war. This aspect is still not recognized in the work on information security of entities. The country, which particularly draws attention to this aspect of information security, is Russia, where extensive research is carried out in this area. As defined by Joanna Darczewska [23], Russian theory of information wars was built as a kind of counterweight to the Western concept of a new generation of wars. Their theoretical assumptions clearly allude to psychological wars run during the Soviet times and the techniques to influence and control society, tried then.

According to theses of J. Darczewska, "in the doctrine of geopolitics information constitutes a dangerous weapon: it is also a low-cost weapon, versatile weapon, with unlimited range, easily accessible, without barriers in the form of state borders. Information and network warfare as well as its extreme forms - war information Psychological and network are the measure to achieve the objectives of the state in international politics, regional and internal, as well as ensuring its geopolitical advantage. The merit of the leading representatives of geopolitical thought is, on the one hand, the popularization of these issues, on the other - personal participation in the wars of information as opinion leaders. This applies especially to the main representatives of the two schools of Russian geopolitics: Igor Panarin and Alexander Dugin, teachers and educators of the young generations of geopolitician. [24]

Gene Sharp (26) also aspires to join the group of adherents of information war. He is the founder of the idea of "velvet revolution" ("refolution (27)") concentrated in the area of strategy for the use of social engineering and information elements in the warfare by revolutionary movements, acting according to his principles. In an environment of specialists, system developed by prof. Sharp is called nonviolent action. Attention should also be paid to the American approach to the problem of information warfare. In the dictionary published by the Department of Defense in February 2001, information war is defined as information activities carried out in times of crisis or conflict to achieve specific goals or to promote them in relation to a specific opponent or opponents [25]. It is worth noting that in the revised edition of the dictionary published in October 2010 (as amended by the release of 2014), the concept of information warfare has been removed, but information warfare was mentioned in other definitions.

A convergence of views can be seen with representatives of leading US information warfare theory, for example - M. Libicki [26] believes that the information warfare as an independent form of warfare does not exist. There are however several separate forms, each of which can be considered as a general concept of information warfare. Libicki describes seven forms of information warfare. These forms include the struggle for dominance in command, based on knowledge and electronic warfare, psychological, economic, cyber war and hacking. While another representative of this trend, R. Szafrański, assumes that the information warfare is a form of conflict, where direct attacks on information systems are a means to attack the knowledge and beliefs of the opponent. According to R. Szafrański information warfare may be conducted as a component of comprehensive hostile activities in the form of network war (NetWare), cyber war, or as a standalone form of fighting. [27] J. D. Arquilla and Ronfeldt state, however, that the information warfare is nothing but using the information to achieve the objectives of the organization. They assume that the information is a key element of the power of the organization, its main resource that supports diplomacy, military violence and the fight for dominance in economy. Information warfare can therefore be seen as a conflict between the entities run in a global information infrastructure. [28]

How can we define the information warfare, having in mind its qualitatively new level? In the fight for information between entities and with information in today's reality, does propaganda begins to dominate with its social engineering aspects? Keeping in mind the nature and duality of information, whereas information processes in the area of security of organization and the associated features, it can be assumed that:

The information warfare (war) is a mutual cooperation (positive or negative) of political actors (players) conducted in the area of security of entities. In the information warfare the object of the impact is a human being and any organized human activity, and its essence is to fight "with" and "for information".

In the information processes accompanying this warfare, in the conditions of deliberately disrupted mapping signals carrying information, it becomes a leading factor of dysfunction, destruction and chaos, leading to critical changes in the area of security of organizations.

Tool for information warfare include, qualitatively new propaganda, using hypermedia. This tool is used by political elite (including, the heads of all faiths and religions) to acquire, exercise and maintain power (or in world of religions - the domination of "their" values) according to their own subjective aspirations and needs, in the name of objective interests of the organization they represent, or intend to represent (28).

7. CONCLUSION

The article proposes a qualitatively new approach to concepts such as: information, area of information security, information security and the information war (warfare). Considerations in this regard have been enriched with a qualitatively new approach to the paradigms of both the information and the information security. Presented interpretation does not imply denial of the achievements of Polish and foreign thoughts related to the theory of information security (IS), at its core lies the thesis of the need to specify the contemporary and projected essence of information security of organization with the growing necessity of generating skills and tools necessary for its (IS) occurrence. Diagnosis of processes and information systems of the organization in the struggle "with" and "for information" has been focused on praxeological terms of the warfare itself, especially in its unarmed form, as the climax of a negative cooperation in the area of security, of which information is immanent component. Not shown here are problems with organizing information warfare, but only those aspects that affect the shape and condition of the organization in the area of information security.

NOTES AND REFERENCES

(1) Area of security of subject - heterogeneous open set consisting of subspace to achieve the goals of actions, for which this space was created, own definition. More: R. Kwećka, Zarys teorii bezpieczeństwa informacyjnego państwa, Warszawa AON, 2013, First chapter.

(2) Process – here understood as " "process of certain changes, successive and causally related, which are stages, phases, stages of development of something; course, development, transformation of something, Słownik języka polskiego, PWN, Warszawa, 1979.

(3) Organization in author's interpretation are countries and international companies, as well as national and foreign political players. Agreeing with L. Krzyżanowski – O podstawach kierowania organizacją inaczej, PWN, Warszawa 1999 - the assumption was adopted that the state is a special organization, governed by the law, it isa subject to other man-made organized action.

(4) The challenges consist of current or future threats and opportunities - it is obvious that every opportunity can become a threat, and each threat may be an opportunity in the security of the state. The estimated value of the challenges to the security of the state is defined in terms of risk. Author's own footnote

(5) or "good" - if one prefers it - because it is a subjective feeling;

(6) Hipermedia – used in one information channel different types of signal, which transmit facts or virtual reality, used for multipurpose interactive influence on the organization – author's own definition, R. Kwećka, Wykorzystanie techniki komputerowej w kształceniu oficerów, AON, Warszawa 2000, p.19.

(7) G. Orwell in his book Nineteen Eighty-Four (1984) published in 1948 (!), "created a" vision of events in our contemporaries and future generations. Events based and carried out on the capacities posed by information processes. His world is constantly unadulterated and "built" from scratch, based on generated on the "demand" of the Ministry of Truth, information about the past - is slowly becoming ours.

(8) Matrix – Australian-American science fiction film, the first of the trilogy of the same name, written and directed by L. and A. Wachowski. The content of the film contains hidden messages and allusions, in which the protagonist, a computer hacker learns from mysterious rebels about the fact that the world in which he lives, is only an image transmitted to the brain by robots. Film image contains many philosophical and religious references, among others, famous Plato's parable of the cave, which is included in the dialogue named "State".

(9) In accepted definition L. Ciborowski focused only on conditional stimulus, which means he treats the stimulus as a factor acting as stimulant by association, rejects the kind of unconditioned stimulus, which acts directly on the senses.

(10) Matter – understood here as "general set of real things existing

objectively, meaning independent of cognition, as well as sensually perceptible; components and systems of this general-called reality, characterized by the extent of the space-time, movement and volatility, in various forms ", Słownik języka polskiego, PWN, Warszawa 1979.

(11) Energy – understood here as „expressed in measures of work scalar physical quantity that specifies the ability of the body or the bodies to work on the transition from one state to another", Słownik języka polskiego, PWN, Warszawa 1979.

(12) The term "control (decision)" system should be understood as the political elite of the organization determining the shape of the area of security.

(13) „Object of influence" – tools of organization useful for shaping the area of security.

(14) Information warfare (IW) – It can be briefly defined as "negative mutual cooperation, at least on two levels, implemented in the areas of: obtaining information, disrupting the information and defending information, where every action of one side is assigned an antagonistic action on the other side", L. Ciborowski, Walka informacyjna, ECE, Toruń 1999, p. 187. Author's qualitatively new approach to IW further below.

(15) Type – understood as –„model, pattern, which corresponds to a series of objects, people, events, forms", Słownik języka polskiego, PWN, Warszawa 1979.

(16) The archetype of these features is contained in: Informacja w walce zbrojnej, R. Kwećka, AON 2001.

(17) Including internal and extrenal subspace of the organization, own footnote

(18) Information Technology – here understood as: hardware and software used for gathering, processing and distrubiuting information (in open or coded channels) together with network systems of communication (internal and external), own footnote

(19) It is commonly believed that the term comes from a science fiction novel Neuromancer by W. Gibson, published in 1984 r.

(20) Mental – concerning the properties of the mind, way of thinking, Słownik wyrazów obcych, PWN, Warszawa 1997); here applicable to society and its mental sphere.

(21) Virtual space should be understood here as a subspace separated from cyberspace. Own footnote.

(22) Mental information is directly conneted with reaction on stimulus.

(23) In 1939, Robert Oppenheimer and Hartland Snyder showed that a massive star may be a part of process of gravitational collapse (collapse under its own weight). As a result of this process, if the star is sufficiently solid, it may shrink to the point of mathematical equations which results from Einstein's work. This idea has not sparked much interest, until the discovery of pulsars in 1967. The name "black hole" was proposed by John Wheeler. Own footnote.

(24) Transformation – change, metamorphosis; math. subordinating element of one set to elements of a given set. Słownik wyrazów obcych, PWN, Warszawa 1997.

(25) "invisible in PURPOSEFUL manner or beacause of the LACK OF KNOWLEDGE, "WEAK"means parts of political elites of countries being SATELITES of certain HEGEMONS, protecting their own SUBJECTIVE interests in the name of OBJECTIVE interests of the nation. Own footnote.

(26) G. Sharp, essay From dictatorship to democracy was first released in Bangkok in 1993 by the Committee for the Restoration of Democracy in Burma, in cooperation with Khit Pyaing (The New Era Journal). Since then it has been translated into at least thirty-one languages, issued in Serbia, Indonesia, Thailand and many other countries. His previous studies have played a significant role in promoting the revolution without violence.

(27) Term „refolution" describes velvet revolutions. It is assumed that Timothy G. Ash was first to use this term in Polska rewolucja. Solidarność 1980-81, Warszawa 1990.

(28) Author's own definition.

[1] R. Kwećka, Informacja w walce zbrojnej, AON, Warszawa 2001.

[2] R. Kwećka, Podstawy bezpieczeństwa.

[3] Stanisław Kamiński, Nauka i metoda – pojęcie nauki i klasyfikacja nauk, Towarzystwo Naukowe KUL, Lublin 1992, p. 24.

[4]R. Kwećka and other authors, Strategie podmiotów. Determinanty zmian, A. Marszałek Publishing House, Toruń 2011, p. 62.

[5]ibidem, p. 27.

[6]L. Ciborowski, Walka informacyjna, p.185.

[7] J. Seidler - Nauka o informacji, Vol I. Wydawnictwo Naukowo-Techniczne 1983.

[8] R. Kwećka, Informacja w walce zbrojnej, Warszawa 2001, p. 31.

[9] R. Kwećka, System ochrony informacji niejawnych [in:] W. Kitler, System bezpieczeństwa narodowego RP

[10] R. Kwećka, Strategia bezpieczeństwa informacyjnego polistrategią bezpieczeństwa podmiotu, [in:] Metodologia badań bezpieczeństwa narodowego. Bezpieczeństwo 2010, P. Sienkiewicz and other authors, AON 2010.

[11] J. Kukułka, Problemy teorii stosunków międzynarodowych, PWN, Warszawa 1978, p. 125.

[12] G.J. Rattray, Wojna strategiczna w cyberprzestrzeni, NT Publishing House, Warszawa 2004, p. 30.

[13]T. Kuhn, Struktura rewolucji naukowych, Fundacja Aletheia, Warszawa 2001, pp. 34-36, 88-100.

[14] K. Darwin, O pochodzeniu człowieka, Jirafa Roja 2009, [via:] J. Gryz, Zarys podstaw teorii bezpieczeństwa. Skrypt wykładów, Warszawa 2010.

[15] K. Mannheim, Ideologia i utopia, Wydawnictwo Test, Lublin 1992, pp. 31-83, [via:] J. Gryz, Zarys podstaw teorii bezpieczeństwa. Skrypt wykładów, Warszawa 2010.

[16] B. Czarnecki, W. Siemieński, Kształtowanie bezpiecznej przestrzeni publicznej, Difin, Warszawa 2004, p. 11, [via:] J. Gryz, Zarys podstaw teorii bezpieczeństwa. Skrypt wykładów, Warszawa 2010.

[17] J. Świniarski, W. Chojnacki, Filozofia bezpieczeństwa, AON, Warszawa 2004.

[18] P. Adriaans, J. van Benthem, Philosophy of Information, T. 8, The Handbook The Philosophy of Science, Elsevier B.V., 2008; access: http://books.google.pl/books?id=lTY00 qJfHnAC&pg=PA24&dq=Adriaans,+Benthem&hl=pl&sa=X&ei=pLP0U6qJMceE4gT4-YD4Dw&ved =0CEwQ6wEg#v=onepage&q=Adriaans%2C%20Benthem &f=false.

[19] M. Lubański, Od informacji ku mądrości, KUL, „Roczniki Filozoficzne", vol. 52, no. 1, pp. 27-40.

[20] S.W. Hawking, Information Preservation and Weather Forecasting for Black Holes, Cornell University Library, 22 Jan 2014.

[21] http://wyborcza.pl/1,75400,15337178,Stephen_Hawking__czarnych_dziur_nie_ma.html#ixzz3B6t WoyFc.

[22] R. Kwećka and others, Strategie podmiotów. Determinanty zmian, A. Marszałek Publishing House, Toruń 2011.

[23] J. Darczewska, Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku, Punkt widzenia Vol. 42, OSW, Warszawa, 2014.

[24] ibidem, p. 7.

[25] Joint Publication-02, Department of Defense Dictionary of Military and Associated Terms.

[26] M. Libicki, What is Information Warfare? NDU, Washington 1995.

[27] R. Szafrański, Cyberwar: A Theory of Information Warfare: Preparing For 2020, [in:] A. D. Campen, D.H. Deart, R.T. Goodden, Cyberwar: Security, Strategy, and Conflikt in the International Press, Fairfax 1996.

[28] J. Arquilla, D. Ronfeldt, Cyberwar is Coming, [in:] Comparative Strategy vol. 12-1993.