NOVEL INTERPRETATION OF INFORMATION OPERATIONS IN TODAY'S CHANGED OPERATIONAL ENVIRONMENT

Zsolt HAIG
haig.zsolt@uni-nke.hu

NATIONAL UNIVERSITY OF PUBLIC SERVICE, BUDAPEST, HUNGARY

ABSTRACT

The study presents a novel interpretation of information operations due to changes of military operations and operational environment. It analyses the concepts of information operations of NATO and the great powers. Based on these, it creates a comprehensive definition of information operations and categorizes their capabilities. The paper presents the interaction between the technical and cognitive capabilities of information operations and the role and weight of these capabilities in traditional military operations and during the 4th generation military operations in a civilian environment.

KEYWORDS:

Information operations, information superiority, cognitive influence

1. Introduction

The theory and practice of information operations has evolved significantly over the past 25 years. In the middle of the 20th Century, because of the unfolding information revolution, the information technology has now become a determinant of everyday life and a fundamental driving force of social, economic and military development. The increasing use of this technology has significantly contributed to the strengthening of the role and importance of information, which has also affected the transformation of military operations.

In the course of military operations, the exploitation and protection of friendly information management and decision-making capabilities, as well as the weakening of the adversary's information capabilities became increasingly important. This recognition has resulted the development of information operations as a new operational capability. Initially the United States, and later more and more countries, including Russia and China, as well the NATO developed their own information operations concept.

Threats in the information environment are becoming more and more

DOI: 10.2478/bsaft-2020-0013

diverse, and their interaction can increase their effectiveness. The information operations that emerged in the '90s have now undergone a significant transformation. This transformation is generated by the changed environment of military operations, the emergence of new technologies, and the transformation of cyberspace.

Based on all this, the aim of this study is to point out the different approaches of information operations in traditional and 4th generation military operations, and to interpret information operations in a novel approach in the changed operational environment, as well as to present their information capabilities.

2. Information superiority and cognitive influence

Thanks to advances in infocommunication technology, early views on coordinated information activities have approached information operations primarily from a technical perspective. The focus of initial information operations theories was on acquiring, maintaining, and exploiting information superiority in the leadership and management process.

This traditional information superiority can be interpreted in classical military operations, where differences in infocommunication technology capabilities between opposing parties are essential to the success of operations. As a result, this approach is fundamentally technology-centric and focuses on the efficiency of collection, storage, processing, and transmission of information. In this case, information superiority applies in most cases to the full spectrum of military operations. The goal of building information superiority is to make friendly decision-making faster than that of the adversary and to provide valid and relevant responses to handle the operational situation.

However nowadays warfare has changed, 4th generation warfare has emerged, and the range of people involved in operations has expanded and transformed. Thus, gaining information superiority as a primary goal has also changed. In today's military operations, coordinated information activities are often carried out in a civilian environment, towards neutral stakeholders and the population. In this case, the goal is not to have more or better information for friendly forces, or to make better use of it, but to win over the target audience for the purposes of military operation. According to some theories, from this approach information superiority cannot even be interpreted in a civil environment. However according to other interpretations for example the one based on Great Britain's information superiority doctrine – information superiority can be interpreted in the following dual approach, depending on the nature of military operations:

- traditional information superiority (between friendly forces and adversaries, mostly in classic military operations);
- adaptive information superiority (JDN 2/13, 2013) (Rózsa, 2016).

Unlike traditional information superiority, the adaptive approach is basically non-technical. Instead of, it means gaining tactical information superiority over the other party that also results in global effects. In many cases, this can be achieved by influencing and manipulating the target audience, which can often be more effective than using technical means. According to adaptive information superiority, influencing non-state actors, neutral stakeholders, and the population is also an important factor in today's military operations. In this case, the aim is not to achieve a literal superiority over these actors. Rather, the information activities – mainly in the cognitive dimension – are

aimed at continuously conveying messages to these actors that can influence them in accordance with the objectives of the military operation. As a result, importance of cognitive information activities increases in these operations.

3. Doctrinal interpretations of information operations

Recognizing the change in the nature of military operations after 2010, the United States re-evaluated its previous position and views on information operations. In the recent U.S. Joint Information Operations Doctrine (Joint Chiefs of Staff, 2014) the importance of human influence is recognized, so the cognitive dimension is considered as the most important component of the information environment. According to the doctrine, information operations are "*the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.*" (Joint Chiefs of Staff, 2014, I-1).

As you can see, the goal is to influence the enemy and your own decision-making process. The doctrine focuses on the target audience selected for influence in the information environment. This is a good indication of the paradigm shift in the appreciation of the role of cognitive information capabilities. Another important recognition is that doctrine specifically highlights cyberspace in the information environment as a new operation area (Joint Chiefs of Staff, 2014).

NATO renewed the AJP 3.10 information operations doctrine in 2015. The new doctrine highlights that unconventional operations, asymmetric warfare come to the front, and the importance of non-state actors becomes more important. In defining the doctrine, "*Info Ops: a staff function to analyze, plan, assess and integrate information activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries and NAC approved audiences12 in support of Alliance mission objectives. Information activities: actions designed to affect information or information systems. Information activities can be performed by any actor and include protection measures.*" (NATO, 2015, 1-5).

The new doctrine also focuses on the will, understanding and capabilities of the individuals involved in operations and defines the essence of information operations in terms of their impact on them. The doctrine distinguishes three interrelated areas of information operations.

These are:

- preserving and protecting one's own information activities in the information environment;
- influencing and/or strengthening the behaviours, perceptions and attitudes of NATO-approved actors;
- countering an adversary's propaganda as well as their command and control (C2) functions and capabilities (NATO, 2015).

NATO doctrine lists and briefly describes all capabilities and techniques that are integrated into information operations.

These are:

- psychological operations;
- electronic warfare;
- civil-military cooperation
- computer network attack;
- computer network protection;
- presence, posture, profile;
- deception;
- operational security;
- key leader and soldier-level engagement;
- physical destruction;
- public affairs (NATO, 2015).

All of the listed capabilities and techniques are information activities, however, in some cases this categorization is not exact, because there are several overlaps between them. Examples include the separation of psychological operations, key leader and soldier-level engagement as well as the presence, posture, profile capabilities. If we think about it, we can see that all these three capabilities affect the thinking, motivation and behaviour of people, which is the essence of psychological operations. The presence, profile and hostile or friendly behaviour of a military organization can have a significant psychological impact on both the enemy and the neutral stakeholders. So these can also be classified as psychological operations.

Another example is to list computer network attack and computer network protection separately. These activities, complemented by computer network reconnaissance, can be interpreted as computer network operations in the same way as electronic warfare, which also has intelligence, offensive, and defensive aspects. Therefore this kind of categorization is not sufficiently structured and does not reflect a systems-based approach to capabilities.

At the same time, the positive elements of the doctrine is that it interprets the information environment in detail and highlights the importance of the impact and role of networked information technology, mobile infocommunication tools, as well as the internet and social media. All of this predicted the inclusion of cyberspace in the dimensions of military operations, which was also formally done at the 2016 NATO Summit in Warsaw. The heads of government of the member states have adopted cyberspace as the fifth dimension of military operations alongside land, air, sea and space.

Russia also pays special attention to operations in the information space. Russian views approach the information war (Russia uses the terminology of information war (информационная война) or information confrontation (информационное противоборство) instead of information operations) from an information technology and information psychology perspective. The information technology side means attacking or defending information systems by technical means using methods of radio electronic combat (russian term for electronic warfare) and computer network warfare. The information-psychological side is aimed to influence and manipulate the thinking, behaviour and emotions of the adversaries, the public opinion and the masses in the cognitive domain, to obstruct decision-making processes, and ultimately to create positive political effects (Thomas, 2004).

In 2013, Army General Valery Gerasimov, Russia's Chief of General Staff, explained in a study that the information space offers great possibilities for asymmetric capabilities that can significantly limit an enemy's combat potential (Gerasimov, 2016). The ideas formulated by the Chief of Staff fit well with Russian Federation Armed Forces' Information Space Activities Concept, which consider the information war as a confrontation between states in the information space. According to the definition of the strategic concept: "*Information war is the confrontation between two or more states in the information space with the purpose of inflicting damage to information systems, processes and resources, critical and other structures, undermining the political, economic and social systems, a massive psychological manipulation of the population to destabilize the state and society, as well as coercion of the state to take decisions for the benefit of the opposing force.*" (Russia Infospace Activities, 2012).

The concept emphasizes that the Russian Federation Armed Forces must

exploit the cutting edge cyberspace technologies, tools and methods. In recent years, recognizing the importance of internet news portals, blogs, and social media, Russia has discovered a new field of cognitive influence in cyberspace. Therefore, these new media platforms are being used intensively to achieve strategic, political and military goals. With the information (often with false news) conveyed through them, they reach masses of people whose conscious activities, thinking, opinions are influenced and manipulated according to their own goals.

China defines information warfare as a basic battlefield capability as a series of operations in the information environment. The basic forms of it are electronic warfare and computer network warfare against military infocommunication systems. The importance of electronic warfare and computer network warfare is well illustrated by the fact that the combined application of these two activities is reflected in a concept of "*Integrated Network Electronic Warfare*" (Anand, 2006).

This perception also appeared in China's National Military Strategy, which was issued in May 2015. The strategy emphasizes that today the international strategic challenges are becoming more and more intense in cyberspace as well. Therefore, China will accelerate the development of cyber forces, increase cyber situational awareness and cyber defence, ensure national network and information security, and participate in the international cyberspace cooperation (Kanwal, 2017).

Information warfare in the cognitive dimension is interpreted in the same way as other forces. In this regard China uses similar approach as the US and NATO. These activities are considered applicable in both peace and war conflicts. The influencing activity in the cyberspace also arises in Chinese thinking, but it does not appear as markedly as e.g. in the Russian information confrontation strategy. Instead of, they focus on traditional psychological operational tools and procedures, and see important opportunities in misleading decision-makers (Anand, 2006).

4. A novel comprehensive approach of information operations

Based on the analysis and synthesis of the presented doctrines and strategies, a comprehensive definition of information operations can be determined that is valid for today's changed operational environment. Information operations are a set of activities aimed at the integrated, synchronized and coordinated application of information capabilities in the information environment, which create desired effects on the will, understanding and capability of the target audience directly with cognitive capabilities and/or indirectly with technical capabilities to achieve the objectives of the operations.

The above comprehensive definition interprets the operational domain of information operations, emphasizes its integrative and coordinating function, defines its overall objective and the two main groups of information capabilities, as well as its target audience. The interpretation of information operations by definition is illustrated in Figure no. 1.

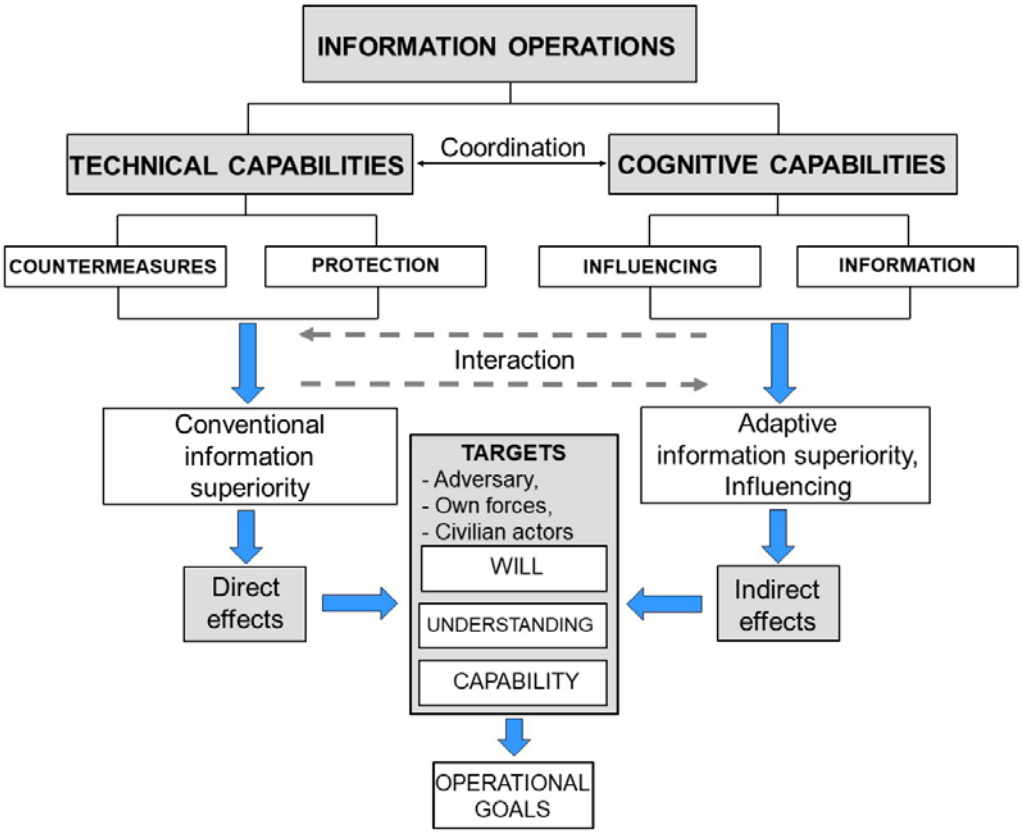

Figure no. 1: *Comprehensive interpretation of information operations*
(Source: Author)

The operational domain of information operations is the information environment in which physical, information and cognitive dimensions can be interpreted. Nowadays, the previous, mainly technical approach of the information environment has been re-evaluated, and the significance of the direct information effects on the target audience in the cognitive space has increased. This is especially true for the 4th generation military operations in a civilian environment.

In addition, due to the rapid spread of networked infocommunication technology, the cyberspace is an increasingly important and significant domain of this environment and it affects all three dimensions of the information environment. Effects in the cyberspace occur not only in the computer network environment, but also in the full spectrum of cyberspace technologies, like e.g. cyber-physical systems and in the people's cognitive capabilities thanks to the online media and social network.

The targets of information operations always depend on the nature of the operations, but basically they can be divided into three broad groups:

- opposing party, or adversary;
- own forces and;
- civilian actors.

In the 4th generation military operations, where there are often no obvious enemies, the primary target group is civilians. In terms of the information operations that can be applied to them, it is useful to distinguish between:

- the non-state actors, irregular forces or armed groups involved in the military operation, and
- the population living in the area of operation.

Against the first group, the use of offensive information capabilities achieving

negative effects is also acceptable and often expedient. However, it is advisable to carry out information operations towards the population, which help to gain their trust and sympathy, and as a result, they accept the goals of the operations and do not hinder in their achievement.

The general goal of information operations is to support military operations in an information environment. Depending on the nature, environment and target audience of military operations, this general goal can be achieved by creating information superiority and/or influencing effects. As mentioned earlier, traditional information superiority over the enemy can be interpreted as an information operation goal and mostly in war conflicts. Traditional information superiority supposes that the opposing party has an adequate quality information infrastructure and infocommunication systems. Through these, their information management and decision-making capabilities can be effectively limited. In addition, cognitive influencing techniques can be applied directly to them to achieve information superiority, so the interaction between technical and cognitive capabilities prevails.

In the 4th generation military operations, the model of the classical achieving of information superiority cannot be fully applied, because civilians also play a significant role in these operations. In these operations, the development of adaptive information superiority may be expedient. In this case, the emphasis is not necessarily on the more advantageous information management and decision-making capability of one's own forces, but on the transforming the thoughts, opinions, behaviour and attitudes of the target audience as well as on their convincing and influencing. Consequently, indirect information technical methods are often less applicable these kind of operations. Among others, due to this fact is that adaptive information superiority better emphasizes the role of cognitive influencing capabilities that directly affect the target audience. At the same time, if there are appropriate infocommunication infrastructures in the area of operations, indirect information technical methods can also contribute to the development of adaptive information superiority. In this case, an interaction between cognitive and technical abilities can also be observed.

This is because if this target audience has access to the internet and uses social media, the direct influencing effect can reach them more effectively through these cyberspace media. All of these effects can be amplified by the spread of fake news on internet news portals and social media, which can significantly reshape the opinions of individuals. The use of fake news is very payable for their distributor from a social, political, military and marketing point of view, and today there is no doubt about their effectiveness. As a result, the spread of fake news on the World Wide Web and social media is unstoppable for the time being.

5. Capabilities of information operations

In order to achieve the goals described above, various synchronized and coordinated information capabilities are used toward the specific target groups. These information capabilities are integrated into information operations and they can be divided into the following two major groups in terms of information dimensions of implementation and achieved effects:

- technical capabilities;
- cognitive capabilities.

Technical capabilities focus on information management processes, i.e. information collection, storage, processing, and transmission. These capabilities have an indirect effect on the target audience using infocommunication technology and infocommunication systems. Consequently, their direct targets are always infocommunication systems, networks and

their elements. Technical capabilities exert their effects in the physical and information dimensions of the information environment. In terms of their purpose, they may be activities against the adversary's information systems, or activities to protect their own information systems.

In contrast, cognitive capabilities focus on the content of information. In the application of these capabilities, a variety of medium and methods are used, and they directly target people's conscious activities with well-structured messages. Accordingly, the target of cognitive capabilities is always the human, so their effects are in the cognitive dimension of the information environment. In terms of their purpose, these capabilities can be positive, negative and neutral influencing and informative activities.

Positive influence is realized in the form of affirmative messages towards our own forces and the civilian population that sympathizes with us. Negative influencing usually works with warning, threatening, or often misleading messages. Its target groups are the enemy and non-state actors, e.g. irregular forces. Neutral influence exerts its impact through attractive messages to neutral stakeholders that accept operational goals.

In a general approach, the technical and cognitive capabilities of information operations include the following:

- technical capabilities:
- electronic warfare;
- computer network operations;
- physical destruction of information targets;
- technical capabilities of operation security;
- technical capabilities of deception;
- cognitive capabilities:
- psychological operations;
- civil-military cooperation;
- public affairs and mass communication;
- cognitive capabilities of operation security;
- cognitive capabilities of deception (Figure no. 2).

Today's information operations doctrines basically focus on the integration, coordination, harmonization of information capabilities, as well as the analytical, evaluative, planning, and organizing activity, as a staff function. In addition to emphasizing the integrative function of information operations, the role and importance of different information capabilities are also important; because of their coordination is the essence of information operations. However, the doctrines in contrast to the concepts of initial information operations, place less emphasis on their importance and explanation.

This kind of categorization of information capabilities of information operations separates technical and cognitive capability groups. This classification is fundamentally in line with NATO doctrine, but in this systems-based approach the characteristics, tools, methods, and effects of each capability can be clearly defined and distinguished. Technical capabilities indirectly affect the target audience through counteraction and protection methods. On the other hand, cognitive capabilities reach the target audience directly using positive, negative, or neutral influencing techniques, informational tools and methods.

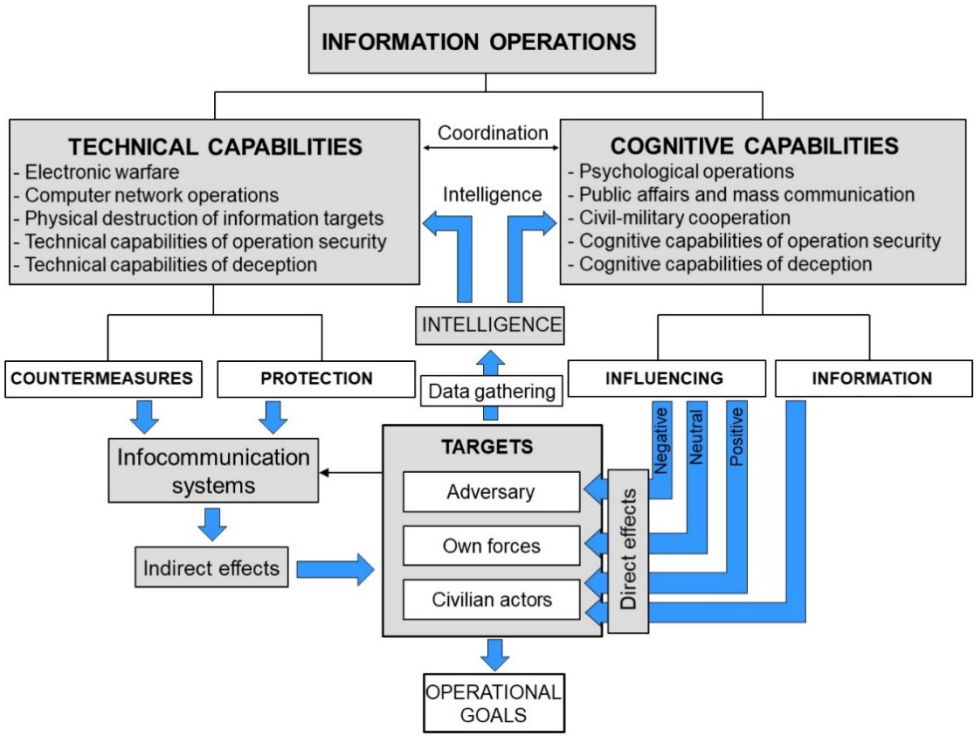

Figure no. 2: *Information capabilities of information operations and their effects*
(Source: Author)

Procedures for almost all information capabilities (e.g., psychological operations, electronic warfare, civil-military cooperation, deception, etc.) are usually contained in separate doctrines. With the exception of operation security and deception, each capability can be clearly classified into either a technical or cognitive capability group based on their tools and methods. These capabilities have long been part of military operations and their functions, tools, and methods are well known.

However, operation security and deception can be found in both information capability groups, because of both have technical and cognitive aspects. Deception can be accomplished by technical means such as using imitated devices, dummies, disinformation communication, electronically simulated targets, spoofing techniques, deceptive software, etc. Cognitive deception includes e.g. fake news that can be effectively disseminated in cyberspace via the internet nowadays.

Operation security, whose function is to protect its own critical information, can also be classified into both information capability groups. The various electronic information security solutions are typically technical information activities. However, the selection and control of individuals handling critical or classified information, or the counterintelligence, are more likely to be cognitive activities.

Nowadays, information operations have become an unavoidable factor in all kinds of military operations. Due to the importance of the role of information, the military capability enhancing, effect increasing and force multiplier role of these operations are unquestionable. The coordinated and integrated application of technical and cognitive capabilities appropriate to the operational environment and target audience ensures that the objectives of information operations can be achieved and thus the successful support of military operations.

6. Conclusions

Information threats to infocommunication networks and the target audience come from the information environment and protection also takes place in this environment. According to the military interpretation, in this environment complex information activities are carried out in the system of information operations. For the past more than 20 years, the initial principles, capabilities, and forms of information operations have undergone constant transformation. At the same time, the essence of this type of military operation has not changed, so the coordination and integration of different information capabilities is still now the essence of information operations.

However, the changed operational environment, 4th generation warfare, and the emergence of civilian actors have had a significant impact on changing the relative roles of technical and cognitive information capabilities. The essence of change is that the philosophy of previous, primarily technical-based information operations has changed, and today the importance of cognitive capabilities is as important as technical capabilities. Another important change is that due to the proliferation of networked technologies, cyberspace is playing an increasingly important role in information operations in point of view of both technical and cognitive information capabilities.

In conclusion, based on the evolution of network technologies, changes in the operational environment and the development of information operations, it can be justified that today the concept of information operations has changed, its technical and cognitive capabilities have become equal and expanded, and the efficiency of information operations can be increased by exploiting their interactions.

REFERENCES

Anand, V. (2006). Chinese Concepts and Capabilities of Information Warfare. *Strategic Analysis, Vol. 30, No. 4*.

Gerasimov, V. (2016). The Value of Science is in the Foresight. New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations. *Military Review*.

Joint Chiefs of Staff. (2014). *Join Publication 3-13. Information Operations*. 27 November 2012. Incorporating Change 1, 20 November 2014, available at: https://fas.org/irp/doddir/dod/jp3_13.pdf.

Kanwal, G. (2017). Acupuncture Warfare: China's Cyberwar Doctrine and Implications for India. *Indian Defence Review*, available at: http://www.indiandefencereview.com/spotlights/acupuncture-warfare-chinas-cyberwar-doctrine-and-implications-for-india/

Ministry of Defence, Development, Concepts and Doctrine Centre. (2013). *Joint Doctrine Note 2/13 (JDN 2/13) Information Superiority.*

North Atlantic Treaty Organization (NATO). (2015). *Allied Joint Doctrine for Information Operations AJP-3.10.*

Rózsa, T. (2016). *Az információs műveletek vizsgálata, különös tekintettel a befolyásolási képességek alkalmazásának lehetőségeire a Magyar Honvédség feladatrendszerében.* PhD dissertation, National University of Public Service, Budapest.

Russian Infospace Activities. (2012). *Russian Federation Armed Forces' Information Space Activities Concept,* available at: http://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle

Thomas, T. L. (2004). *Comparing US, Russian, and Chinese Information Operations concepts,* available at: http://www.dodccrp.org/events/2004_CCRTS/CD/papers/064.pdf