Ann. Disaster Risk Sci. 2019, 1-2, 49-59

CONCEPTUALIZATION OF INFORMATION OPERATIONS IN MODELLING THE UNDERSTANDING OF A SECURITY ENVIRONMENT

Dario Malnar[1], Tomislav Dokman[2]

[1]Croatian Defence Academy "Dr. Franjo Tuđman"

[2]Faculty of Humanities and Social Sciences, University of Zagreb

Abstract

The definition of a security environment, which is a prerequisite for the process of defining security policies, is based on the gathering and evaluation of information on the political, economic, military, security, social and other characteristics of a given environment. The process of gathering and evaluating information is increasingly susceptible to external influences and manipulations via information operations of state and non-state actors, particularly with the development of information technologies. The hypothesis of this paper is that information operations influence the understanding of a security environment and consequently the process of defining security policies. Based on the described hypothesis, the paper conceptualizes information operations in the modelling of the understanding of a security environment and consequently the determination of security policies, using an analysis of certain aspects of information operations and their influence on the information and information systems of the adversary.

Keywords: information operations, security environment, security policies

Address for correspondence: Tomislav Dokman, mag.cin., PhD student of Information and Communication Sciences, Faculty of Humanities and Social Sciences, University of Zagreb, email: dokman.tomislav@gmail.com

INTRODUCTION - SECURITY ENVIRONMENT AND DEFINING SECURITY POLICIES

All states, societies and individuals continuously observe the environment, gather information on it and the evaluation of that information with the goal of determining threats arising from such environment. The states likewise determine the opportunities and possibilities within the environment. Threats and possibilities are continuously determined between each other and the realisation of a possibility usually depends on the successful recognition, understanding and management of threats. Therefore, the goal of states, societies and individuals is to reduce threats, strengthen the security in order to secure more favourable conditions for the realization of possibilities and ensure the conditions for survival as the ultimate goal of every community and individual.

Tatalović et al. write that security activities involve a double relationship: the human-to-human one and the one between the humans and nature.

In this sense, we distinguish two components of such activities:

a) man's immediate reaction to the state and processes within nature and to the situations in society which he sees as a threat;

b) man's understanding of phenomena and processes in nature and society and his preparation for protection and defence against the processes and phenomena that he sees as a potential threat. (Tatalović et al., 2008: 7).

Based on the above, it follows that the prerequisites of security activities are the following:

1. Knowledge of the states and processes in nature and the social conditions, i.e. knowledge

of the security environment in the external and internal contexts - assessing the security environment.

2. Assessing which of these states, processes and situations represent a threat – which gives rise to the need for defining, qualifying and quantifying threats and risks arising from them.

Based on the claim that "the primary condition and goal of every state politics is the survival of the state and society, and the prerequisite for the survival of the state and society is their safety", and the claim that this "represents the framework of security policy, which aims to create an organization for the achievement of internal and external security of state and society, i.e. national security" (Tatalović et al., 2008: 17), it can be determined that knowing and understanding the security environment is the precondition for security activities - security policy and security systems. In addition, it can be said that the definition of these strategic aspects of national security is determined by the characteristics of the security environment and the knowledge and understanding of these characteristics. Therefore, it is clear that our understanding of the components of the security environment must reflect the reality in a realistic and fact-based manner, in order for its interpretation to be as close as possible to the actual factual state. This is not an easy condition to meet. On the one hand, the reason for this lies in the increasing complexity of the security environment within which numerous more or less recognizable and measurable subjects and factors are active. On the other hand, there are the complex workings of different state and non-state subjects who have an impact on the security environment with the goal of realising their own interests. They distort the information on the environment and strive for encouraging the creation of distorted images and wrong conclusions of other subjects regarding a certain aspect of the security environment. These activities are conducted through various hybrid actions. In order to understand the environment, these actions can largely be summarized as information operations, whereas the scope of potential action is considerable.

As has been mentioned above, the security environment has its internal and external context. Apart from the physical one, this context can also be cybernetic. With the help of modern information technologies and tools, this opens up additional space for information activities aimed at determining the understanding of the security environment.

The external environment consists of the external space surrounding a certain subject. In the context of national security, this subject is most often the state, with a whole array of characteristics: physical, normative, procedural and institutional, as well as cybernetic. On the other side, the internal environment consists of characteristics adherent to the state itself, humans, institutions, as well as normative, material and other characteristics, which act as determinants of security definition and action. Thereby, different aspects are analysed - political, economic, military, security, environmental, demographic etc.

Knowledge of the security environment is an activity by which the state is continuously engaged through its various institutions. It is also an activity that is defined through gathering, analysing and evaluating data on the characteristics of the environment. Whether the data on the environment comes from secret sources or through publicly available sources, this data may be subject to manipulation and distortion of facts by a third party.

By correlating the characteristics of the security environment and the basic national values, interests and goals, we define threats to national security,[1] i.e. those manifestations and states

1 For more on the definition of the term ***national security*** see Tatalović, S et al., Suvremene sigurnosne politike, Golden marketing and Tehnička knjiga, Zagreb, 2008, pg. 19 – 22

which can jeopardize national security.[2] We can evaluate the established threats to national security according to the probability and potential consequences. We determine the risk, the "potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences" (Department of Homeland Security, 2010). "Risk can be defined as the combination of the probability of an event and its consequences" (ISO/IEC, 2008). Such established, described and evaluated environment is the prerequisite for defining strategic safety and political aspects - documents, processes and systems.[3]

What is required in order to conduct the whole process is extant data, continuous updating of data on the evolving environment and verified and safe databases. With the development of technology, databases have predominantly switched to electronic media. Electronic media are characterised as "such that there is a danger of tampering with documents and data that are of critical importance for certain societal and business projects" and it is "possible to access resources without leaving a trace, both in theory and practice." (Đorđević, 2007: 71). It clearly follows that gathering and analysing data and consequently drawing conclusions is not enough for an objective understanding of the environment. What is needed is also the safety of information and information systems in which this data is stored, transferred or processed in order to ensure integrity, completeness and accuracy of information.

If we follow Wolfers' example and analyse national security through two aspects - objective and subjective, whereas the subjective is formed by the perception of threat, i.e. the psychological dimension of security which must not be in correlation with the real, objective state of things (Wolfers, 1962: 51), then the potential of information operations in modelling the understanding of security environment gains even more importance. The primary goal and scope of influence of information operations is at this subjective and psychological level of environmental perception and they can govern perception (Dearth, 2002: 1) in order to attain the purpose of information operations, i.e. "the manipulation of public opinion" (Weedone et al., 2017; 4). The ultimate goal is to manipulate the decision-making process.

INFORMATION OPERATIONS AND THEIR GOALS

Information operations stem from the military doctrine of information warfare of the United States Armed Forces (Thusu and Freedman, 2003: 103). Those are the "actions taken to affect the adversary's information and information systems, while defending one's own information and information systems" (Joint Chiefs of Staff, 1998). In the attempt to define information operations, it is necessary to start from the claim that information operations are "essentially the integration of specified capabilities involving information and information systems". The purpose of integrating the said capabilities is "to influence the behaviour of target decision-makers or audiences through the use of information and information systems. Conversely, information operations also seek to shield or defend friendly decision-makers or audiences from being unduly influenced by a target's use of information or information systems (U.S. Army War College, 2006: 1).

These operations are conducted in order "to influence an adversary or potential adversary in support of political and military objectives by undermining his will, cohesion, decision-making ability, through affecting his information, information based processes and systems while protecting one's own decisions-makers and decision-ma-

2 Natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. Department of Homeland Security, DHS Risk Lexicon 2010 Edition, September 2010, Risk Steering Committee.

3 It should be emphasized that the evaluation of the surroundings is not only important at the strategical level, but also on other levels of planning and acting - the tactical and operative one, as well as the activity level of the smallest military entity in a certain environment.

king processes“ (Ministry of Defence UK, 2002).

The influence on decision-makers or audiences encompasses both the influence on the cognitive dimension of understanding a certain phenomenon and the processes of decision-making. Information operations are focused on the ways in which “to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making while protecting our own“ (Joint Chiefs of Staff, 2006/2014). When discussing information systems in the context of information operations, in addition to using them, we are also talking about disrupting, degrading, or destroying adversary information systems. For example, in a strategic document by the Russian Federation, the main offensive and defensive aspects are summarized, and the term *information operations* includes

> *the conflict between two or more countries in the information space, with the purpose of damaging the information systems, resources, strategic infrastructure, undermining the political, economic and social systems, having a general psychological influence on the population with the goal of destabilizing the society and state, as well as forcing the state to reach decisions in the interest of the adversary” (MOD RF, 2011: 5).*

According to the Russian definitions, information operations encompass political, economic, social, military, intelligence, counter-intelligence, diplomatic, propaganda, psychological, information and educational activities (Darczewska, 2014: 10).

The American Military Dictionary defines them as “operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behaviour of foreign governments, organizations, groups, and individuals in a manner favourable to the originator’s objectives” (Joint Chiefs of Staff, 2016: 342).

The ultimate goal of these activities is to gain advantage against the adversary and to secure a victory. Russian theoreticians give information operations a strategic character and the potential for gaining strategic victory. They believe that “in contemporary conditions, the means of information influence have reached the level of development such that they are capable of resolving strategic tasks“ (Chekinov and Bogdanov, 2011, cited in Giles, 2016: 17-19). Apart from the strategic victory, Giles lists the following potential outcomes and goals of information operations:

1) Reflexive control or „the practice of predetermining an adversary’s decision (…) by altering key factors in the adversary’s perception of the world“.
2) Permissive environment „to influence foreign decision-making by supplying polluted information“ with the goal of such information becoming part of the decision-making framework.
3) Subversion and destabilisation, „broad-based, long-term weakening and undermining of adversary societies overall, without necessarily any specific goal than increasing (…) relative strength“, which is conducted by „spreading disinformation among the population about the work of state bodies, undermining their authority, and discrediting administrative structures“ (Giles, 2016, 19-27).

MODALITIES OF INFORMATION OPERATIONS

Even though information operations were initially tied to the American Department of Homeland Security and the US armed forces, with the development of information technologies it became possible for non-governmental subjects and individuals to use them as well (Domović, 2015: 99). The *modus operandi* is the same with state and non-state subjects, considering the fact that they both affect information systems and information as such. It is important to emphasize that strategic communication, public diplomacy and propaganda are not synonyms for information operations (Domović, 2015: 99), but they are predominantly “used by civil institutions” (Hutchinson and

Warren, 2001, cited in Domović, 2015: 99). For example, in order to gain domination in the information space it is necessary to synchronize the use of various tools of strategic communication, i.e. the appropriate messages and purposeful conceptual constructs aimed at a targeted audience (Freeman, 2005: 1). Tools of public diplomacy and public relations likewise need to be used, while minimizing the use of military force and economic sanctions (Larson et al., 2009:2). Information operations can be public in their character, as is the case in strategic communication, public diplomacy and propaganda. Here, the source of information is not concealed, and the secretive properties found in disinformation campaigns and attacks on information systems are not present. Information operations can be used as an autonomous factor of state power or in synergy with other factors, most often as an aspect of hybrid operations.

In his analysis of Russian information operations, Greg Keeley recognizes fake news, wrong information, control over shows and publishing incorrect news via state media, as well as automatized robots on social media which are designed for promoting confusion in the society (Keeley, 2018). As emphasized by Freeman (2005: 1) it is important to bear in mind that for gaining domination in the information space it is necessary to synchronize the use of various tools of strategic communication.

DISINFORMATION ACTIVITIES

Disinformation activities are aimed at establishing a strategic advantage and domination within the information space, primarily by placing non-truths, half-truths or fragments of truths. The carrier of a disinformation operation can be a state or non-state subject or individual. Since disinformation is an important aspect of disinformation operations, it is important to clarify this term, i.e. to pinpoint its multidimensionality. According to Fallis, disinformation includes incorrect information that is disseminated as false information towards the recipient and is published with the purpose of deception. Disinformation exhibits the characteristics of information, deceitful information and targeted deceitful information (Fallis, 2015: 404-408). It is important to stress that any information can imply "truth and lie" (Fox, 1983, Scarantino & Piccinini, 2010, according to Fallis 2015: 405). Considering the fact that a piece of information is descriptive in character, in the event of false presentation, it is clear that its goal is to purposefully shape another person's wrong opinion. This is precisely the ultimate goal of an information operation, i.e. of a disinformation campaign.

In the context of conducting disinformation activities, it is important to emphasize that this involves „spreading of a rumour by means of an orchestrated effort makes it a disinformation campaign (Ferrara 2017:3). Even though rumours and non-truths aim at influencing a target audience and creating a desired corpus of public knowledge, the strategic potential of disinformation campaigns is evident. Campaigns are conducted by means of different communication channels which easily penetrate the space of vulnerable groups. Since disinformation is an integral part of information operations, it is necessary to emphasize that the development of information and communication technologies has enabled an array of possibilities for spreading disinformation that was previously unimaginable. Social media, blogs and forums are the most commonly used platforms for spreading disinformation. All of the above points to a systemic problem in fighting disinformation campaigns, given the fact that – from a practical standpoint - it is very difficult to control large amounts of data being disseminated into public sphere. The difficulties in controlling the spread of disinformation are a key component in acting based on the obtained information. Ladislav Bittman, the former deputy director of the former Czechoslovakian intelligence service, claimed that it is equally important to detect disinformation itself. However, this is extremely difficult to do

as "every disinformation message must partially correspond to reality" (Bittman, 1985 according to Boghardt, 2008: 2). It is clear that said attributes make it more difficult for intelligence institutions to discover disinformation in the mediascape. Vulnerable groups are extremely exposed since they do not possess the safety culture of noticing disinformation campaigns. At the same time, they do not verify the credibility of information sources or the content they publish. These groups are the most common targets of disinformation activities.

Strategic communication

The United States of America consider strategic communication to be:"efforts to understand and engage key audiences to create, strengthen, or preserve conditions favourable for the advancement of United States Government interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power" (Joint Chiefs of Staff, 2016:226).

NATO definition gives additional aspects stating that strategic communication is

"the coordinated and appropriate use of NATO communications activities and capabilities – Public Diplomacy, Public Affairs, Military Public Affairs, Information Operations and Psychological Operations, as appropriate - in support of Alliance policies, operations and activities, and in order to advance NATO's aims" (NATO, 2009: 1).

Strategic communication is conducted in order to provide information to its recipients, but also to increase one's influence and convince the target audience, for the purpose of pursuing national interests. Persons conducting such communication use messages, images and other forms of communication (Kuzelj et al. 2017: 2). It includes the purposeful usage of communication with the goal of achieving a certain task (Kirk Hallahan et al., 2007: 3) in order to "shape perception and change behaviour" (Fink, 2013: 7). In the corporate world, this involves „communication aligned with the company's overall strategy, to enhance its strategic positioning" (Argenti et al., 2005: 61), while in the military context in encompasses the "highest layer within the communication climate" in order to „achieve national objectives" (Perry, 2008: 7). Based on the claim that strategic communication is "the synchronized promulgation of information, ideas and actions over time through means and content that are tailored for audiences" (Goldman, 2008: 5), it can be said that with the aid of strategic communication, one can influence the understanding of the elements of the security environment. In accordance with this and the specifics of their own strategy, the person conducting the operation can advance not only their own interests but complicate the understanding of the security environment and make the defining of security policies more difficult. This is achieved by distorting the interpretation and using false presentation of key elements of the security environment. Therefore, it is claimed that the "aim of Strategic Communications is to make political-military communications more strategic and capable of influencing the target audiences' way of thinking and behaving, by facilitating the rapidity and coherence of the communications" (Reding et al., 2010: 2).

Public diplomacy

Public diplomacy involves the action of one sovereign country towards the general public in other countries, in order to influence the attitudes and opinions of the public in other countries with the goal of accepting and promoting national goals and interests of these countries (Tuđman, 2009: 28). He similarly defined public diplomacy as an "international actor's attempt to manage the international environment through engagement with a foreign public" (Nicholas Cull, 2009: 12). The term *public diplomacy* has changed through time. However, it has remained focused on the impact on foreign audiences and the shaping of public opinion.

In the context of public diplomacy, we can speak of several specific points:

- Public diplomacy is directed at an international / foreign public and it refers to that general public or to certain selected groups within it (…),
- Public diplomacy of an individual state aims to improve the international public opinion about the country itself and the policy which the state conducts,
- Public diplomacy seeks to create conditions for a more effective implementation of policies and the promotion of national interests,
- Public diplomacy seeks to strengthen the national security of a country (Malnar, 2009: 71-72).

These activities also occur in the public sphere. Since they are aimed at gaining a strategic advantage against the target country, it is clear that people conducting such operations are trying to influence the security environment. A point should be made that by relying on truthful data, public diplomacy differs from propaganda. However, due to the easy spreading of disinformation and lies, activities from the sphere of public diplomacy enter the space of synergistic influences when interacting with these aspects of information activities. In this way, they model the security environment and make its understanding more difficult. Consequently, they make the creation of security policies more difficult as well.

Propaganda

Cambridge Dictionary defines propaganda as "information, ideas, opinions, or images, often only giving one part of an argument, that are broadcast, published, or spread in some other way with the intention of influencing people›s opinions" (Cambridge Dictionary, 2018). In his definition, Taylor (2003: 6) emphasizes that these are conscious, methodical and planned decisions for the application of persuasion techniques, designed to attain specific goals which are aimed at users organizing the process. In the first half of the 20th century, Lasswel defined four major propaganda strategies, which are sustainable even today:

1. Stirring hatred towards the enemy.

2. Keep the friendship with allies.

3. Keep the friendship with and, if possible, create a collaboration between neutral actors.

4. Demoralise the enemy (Lasswell, 1938: 195).

The emphasis is on influencing the targeted group in order to achieve a certain goal which is in the interest of the person conducting the propaganda activity. It is important to note that a propaganda campaign can contain untruths and deceitful information in spreading its constructs, in equal measure as a disinformation campaign.

Fake news

Fake news uses fabricated data and its purpose is to create information confusion in the mediascape. It is not based on facts, but rather contains distorted information, just like disinformation and misinformation (Lazer et al. 2018: 1094). Apart from fake news, in the public sphere we encounter fake accounts, fake social media profiles, offers, survey data or data on the voters' inclination towards a political party, candidate or data on the security environment. The said manner of communication with the surroundings becomes a key part of information and security strategies, as well as political and economic campaigns. For example, it is used when companies or states wish to mislead the public with data on successful business or financial gain, while the reality is completely different. Algorithms, i.e. artificial bots are often used in the cyberspace in order to conduct such operations. Bots are the "software that imitates human behaviour" and they represent the "dominant new force in the public discourse" (DiResta 2017). Their activity ensures the spread of contaminating content towards the target population. For example, "nearly 50 million accounts on Twitter are actually automatically run by bot software" (DiResta, 2017). It is hard to imagine the amount of false or distorted data generated by 50 million automated accounts. In this way, the

environment from which the data is drawn becomes less and less useful for creating an accurate and correct account of facts.

Attacks on information systems

When talking about the aims of an attack, information operations can be aimed towards adversary information as well as information systems (Joint Chiefs of Staff, 2006: I-1). Francesca Ferraro claims that an attack on information systems means damage to the crucial infrastructure required for the functioning of the state apparatus, as well as an unauthorized entry into information systems that contain confidential data, as well as the interception of messages without permission. (Ferraro, 2013). Security institutions must make a continuous effort to protect their information systems, but also to detect potential targets of the potential adversary activity, as well as promoting the early warning system. It is therefore clear that "cyber-attacks are more extensive, more sophisticated, better coordinated than hacking attacks and directed towards the adversary's significant goals" (Damjanović, 2017: 1050). It is evident that we are in a vulnerable environment characterized by the danger of malicious attacks aimed at the information space of the targeted country or group. Therefore, we should be asking ourselves of the real danger of cyber-attacks and whether we should be worried about a cybernetic infiltration of another state into the missile system of a third country, or about an illegal initiation of the early warning system which could lead to the missile system being directed towards another country (Blair, 2017). The question is raised in which measure will the development of artificial intelligence influence the implementation and the potential of information operations. The NATO foresight analysis for 2017, published by the Allied Command Transformation, highlights the challenges NATO faces due to the development of information technologies. For example, NATO sees potential challenges in the uneven development of disruptive technologies and the unequal regulatory frameworks in the member states. This leads to problems in the interoperability of forces, but also to the greater opportunity that individuals, state actors and non-state actors have to access and exploit information, as well as smaller groups with bad intentions and the possibility of spreading fake news and increasing the domination of the private sector (NATO, 2017: 8). Therefore, "traditional techniques (e.g. print media, radio, movies, and television) have been extended to the cyber domain through the creation of the Internet and the social media" (Waltzman, 2017: 1). In other words, advanced technologies make it easier to conduct information operations and make them more dangerous than ever before. Joseph S. Nye pointed to the strategic potential of information operations. According to him, the best example is the recent "Russia's interference in the 2016 US presidential election, and its suspected hacking of the_French President Emmanuel Macron's campaign servers". He claims that "cyber technology makes it cheaper, faster, and more far-reaching, as well as more difficult to detect and more easily deniable". (Nye, 2018). An example is the hacker attack in April 2013 when hackers took control of the Associated Press' official Twitter account and tweeted „two explosions in the White House and Barack Obama is injured" (Fisher 2013, according Allen and Chan, 2017: 33). The aftermath was that "in the two minutes following the tweet, the U.S. stock market lost nearly $136 billion in value until the hack was revealed (Wang et al., 2018). Therefore, it is clear that a single piece of fake news can greatly influence the stock prices. For example, potential multiplication of such news would lead to immeasurable consequences with respect to the economic stability of a country. This would subsequently make it more difficult to interpret and define the security environment, particularly the characteristics from the economic sphere. It can be surmised that the development of artificial intelligence, in addition to its positive sides, also bears numerous challenges, particularly in the field of information operations. Artificial

intelligence is becoming capable of performing increasingly complex tasks, particularly in cybernetic warfare. For the information sphere of the development of artificial intelligence, this means an exponential increase in the number of sources of information, gathering data, as well as easier and cheaper falsification of information (Allen and Chan, 2017: 2).

CONCLUSIONS

The modern global environment is characterized by the significant domination of information, where information is not only a signal or a piece of news sent out from the sender to the recipient with the goal of transparently informing the recipient, but also a means of promoting national interests and attaining national goals. Information campaigns are directed towards the achievement of national interests and goals by creating the desired corpora of attitudes within the target population from the scope of their own state corpora or from the corpora of a foreign state.

Since the advent of modern advanced communication applications and online mass communication platforms, the reach of the information-communication process has been demonstrating its additional operative and strategic potential. The Internet and the development of information and communication technologies have enhanced and simplified the global spread of information and warfare conducted using this information.

In addition, the ability to exert influence is now 'democratized' and 'individualized' since every individual, group or non-governmental actor is in the position to communicate and influence large groups of people using the Internet (Waltzman, 2017: 2). The fast spreading of information has enabled individuals, extremist groups, state and non-state subjects to widen their scope of impact and information has become a powerful tool (Joint Chiefs of Staff, 2013: 1). Since information operations have shifted from the traditional media to the virtual sphere, the persons conducting information campaigns increasingly opt for the spreading of disinformation and fake news. We are primarily talking about the use of disinformation campaigns, where the person conducting the activities tries to remain hidden. The same applies to the attacks on the information systems.

The person conducting the activities forms the desired corpora of public knowledge of the targeted group or manages their perception and cognitive domain. The analysis of the forms, content and goals of information operations creates a foundation for the conclusion that information operations have the potential of influencing and managing the individual's and group's perception and that with the placement of targeted constructs one can create a false image of the security environment. In addition, it can be concluded that the development of modern information technologies additionally strengthens the potential to model the perception of the security environment. This potential is brought to a new level with the development of artificial intelligence, which multiplies the ability of data processing and machine generation of narratives, where the role of the individual is reduced to the setting of desired parameters. Reality then becomes a virtual category in which information operations have an increasing influence on the definition of the security environment and its understanding. Consequently, they influence the ability of the carrier of information operations to influence the definition and implementation of security policies and the decision-making process of other countries, based on their own interests. We can therefore agree with the assessment that "[…] the victory in information war can have the same effects and be as successful as a victory in a classical military conflict" (Baluyevski, 2018) and that strategic communication or real journalism and real information are sometimes more important than tanks and war plans in the contemporary world (Keeley, 2018).

BIBLIOGRAPHY

Allen, Greg and Chan Taniel (2017): Artificial Intelligence and National Security. Belfer Center for Science and International Affairs. Harvard Kennedy School.

Argenti, Paul A., Howell Robert A. and Karen A. Beck (2015): The Strategic Communication Imperative, 61-67. In MIT Sloan Sloanselect Collection (eds.), Top 10 Lessons on Strategy.

Boghardt, Thomas (2009): Soviet Bloc Intelligence and Its AIDS Disinformation Campaign, Studies in Intelligence Vol. 53 No. 4 December 2009.

Cull, Nicholas J. (2009): Public Diplomacy: Lessons from the Past. USC Center on Public Diplomacy at the Annenberg School University of Southern California.

Damjanović, Dragan Z. (2017): Types of information warfare and examples of malicious programs of information warfare. Military technical courier, 2017 65 (4): 1044-1059.

Darczewska, Jolanta (2014): The anatomy of Russian information warfare: The Crimean operation, a case study. Point of view. Number 42. Centre for Eastern Studies. Warsavw.

Department od Homeland Security (2010): DHS Risk Lexicon 2010 Edition, September 2010, Risk Steering Committee.

Dearth, Douglas (2001), Implications and Challenges of applied Information Operations. Journal of Information Warfare Volume 1 (3:): 7-15.

Domović, Roman (2015). Metodologija provođenja informacijskih operacija. National security and the future, 16 (2-3): 95-120.

Đorđević, Ivica (2007): Bezbednosna arhitektura u uslovima globalizacije, Univerzitet u Beogradu – Fakultet bezbednosti i Službeni glasnik, Beograd, 2007.

Fallis, Don (2015): What is disinformation? Library Trends,Volume 63 Issue number 3: 401–426, Exploring Philosophies of Information edited by Ken Herold.The Board of Trustees, University of Illinois.

Ferrara, Emilio (2017): Disinformation and social bot operations in the run up to the 2017 French presidential election. First Monday, Peer-Reviewed Journal of the Internet, Volume 22 Number 8 – 7 August 2017.

Giles, Keir (2016): NATO Handbook of Russian Information warfare. Followship Monograph. Research Divison NATO Defense College 9, November 2016.

Hallahan, Kirk, Holtzhausen Derina, van Ruler Betteke, B., Verčić Dejan and Sriramesh Krishnamurthy (2007): Defining Strategic Communication. International Journa od Strategic Communication, 1(1): 3–35.

ISO/TMB WG on Risk management N 066, ISO/IEC Guide 73, Risk management — Vocabulary, 2008.

Joint Chiefs of Staff (1998): Joint Publication 3-13 Joint Doctrine for Information Operations. Joint Pub 3-13, 1998. United States. Joint Chiefs of Staff.

Joint Chiefs of Staff (2006): Joint Publication 3-13 Information Operations. Joint Pub 3-13, 2006. United States. Joint Chiefs of Staff

Joint Chiefs of Staff (2016): Joint Publication 1-02 Departtment of Defense Dictionary of Military and Associated Terms. United States. Joint Chiefs of Staff.

Joint Vision 2020 (2000): America's Military: Preparing for tomorrow. Washington, D.C., US Government Printing Office, June 2000.

Kuzelj, Maja, Dokman Tomislav and Katalinić Josip (2017): Kibernetički napadi i krizno komuniciranje - izvještavanje novinskih portala. MIPRO 2018: 41. međunarodni skup za informacijsku i komunikacijsku tehnologiju, elektroniku i mikroelektroniku Opatija.

Larson, Eric V., Darilek Richard E., Gibran Daniel, Nichiporuk Brian, Richardson Amy, Schwartz Lowell H. and Thurston Cathryn Quantic (2009): Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities. Santa Monica, RAND.

Lasswell, Harold D. (1938): Propaganda Technique in the World War. Chatham: Mackays.

Lazer, David M. J., Baum Matthew A., Benkler Yochai, Berinsky Adam J., Greenhill Kelly M., Menczer Filippo, Metzger Miriam J., Nyhan Brendan, Pennycook Gordon, Rothschild David, Schudson Michael, Sloman Steven A., Sunstein Cass R., Thorson Emily A., Watts Duncan J., Zittrain Jonathan L. (2018.): The science of fake news. Science. Volume 359 Issue 6380: 1094-1096.

Malnar, Dario (2009): Diplomacia publike dhe imazhi ndërkombëtar I Kosovës. Revistë Shkencore: Institute for Security and Integrations Studies, Prishtine, p. 69 – 78.

NATO (2009): NATO Strategic Communication Policy. PO(2009)0141 29 September 2009.

NATO Allied Command Transformation (2017). Strategic Foresight Analysis. 2017 Report.

Perry, Robert L. (2008): Principles of Strategic Communication for a new global commons. Naval War college, Newport, RI.

Reding, Anais, Weed Kristin and Ghez Jeremy (2010): NATO's Strategic Communications concept and its relevance for France. RAND Corporation.

Tatalović, Siniša, Grizold Anton and Cvrtila Vlatko (2008): Suvremene sigurnosne politike. Golden marketing i Tehnička knjiga, Zagreb, 2008.

Taylor, Philip M. (2003a): We know where you are: Psychological operations Media During Enduring Freedom. In Daya Kishan Thusu and Des Freedman (eds.), War and Media. Reporting Conflict 24/7., 101-113. SAGE Publications.

Taylor, Philip M. (2003b): Munitions of the mind: A history of propaganda from the ancient world to the present day. Thir Edition. Manchester University Press.

Tuđman, Miroslav (2009): Informacijske operacije i mediji ili kako osigurati informacijsku superiornost. National security and the future 10 (3-4): 25-45.

U.S. Army War College (2006): Information Operations Primer. AY07 Edition, November 2006, Carlisle.

Waltzman, Rand (2017): The Weaponization od Information: The Need for Cognitive Security. The RAND Corporation.

Weedon, Jen, Nuland Willian and Stamos Alex (2017): Information Operations and Facebook, April 27, 2017 Version 1.0.

Wolfers, Arnold (1962): Discord and Collaboration: Essays on International Politics. Baltimore: Johns Hopkins University Press.

Sources

BBC News (2017): Russian military admits significant cyber-war effort. Accesible at https://www.bbc.com/news/world-europe-39062663 12. 11. 2018.

Blair, Bruce G. (2017): Why Our Nuclear Weapons Can Be Hacked. The New York Times. Accesible at https://www.nytimes.com/2017/03/14/opinion/why-our-nuclear-weapons-can-be-hacked.html?mcubz=1&_r=0 , 30. 11. 2018.

Cambridge Dictionary (2017): Propaganda. Accesible at https://dictionary.cambridge.org/dictionary/english/propaganda, 29. 11. 2018.

DiResta, Renee, Little John, Morgan Jonathan, Neudert Lisa Maria and Nimmo Ben (2017):The Bots That Are Changing Politics. Motherboard. Accesible at https://motherboard.vice.com/en_us/article/mb37k4/twitter-facebook-google-bots-misinformation-changing-politics, 23. 11. 2018.

Ferraro, Francesa (2013): Attacks against information systems. Library Briefing Library of the European Parliament. Accesible at http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2013/130571/LDM_BRI(2013)130571_REV1_EN.pdf, 29. 11. 2018.

Goldman, Emily (2008): Strategic Communication Theory and Application. II.10.2018. Accesible at http://www.naylornetwork.com/jed-nxt/Goldman_Plenary.pdf, 2. 10. 2018.

Joint Warfare Publication 3-80 (2002): Information operations. Ministry of Defence UK. Director General, Joint Doctrine and Concept. Accesible at http://www.stratcomhellas.weebly.com/uploads/5/1/6/5/51658901/jwp3_80_uk_info_ops_doctrine.pdf, 8. 10. 2018.

Keeley, Greg (2018): The Hill: Combatting Russian information warfare — in the Baltics. Accesible at https://thehill.com/opinion/technology/382245-combatting-russian-information-warfare-in-the-baltics, 20. 11. 2018.

Ministry of Defence odf Russian Federation (2011): Conceptual views on activity of the armed forces of the Russian Federation in information space. Accesible at http://pircenter.org/media/content/files/9/13480921870.pdf, 11. 10. 2018.

Nye, Joseph S. (2017): Information Warfare Versus Soft Power. Belfer Center for Science and International Affairs. Harvard Kennedy School. Accesible at https://www.belfercenter.org/publication/information-warfare-versus-soft-power, 27. 11. 2018.

Wang, Lu, Kisling Whitney and Lam Eric (2013): Fake Post Erasing $136 Billion Shows Markets Need Humans. Bloomberg. Accesible at https://www.bloomberg.com/news/articles/2013-04-23/fake-report-erasing-136-billion-shows-market-s-fragility 30. 11. 2018.