RIGA TECHNICAL UNIVERSITY

Information Technology and Management Science

ISSN 2255-9094 (online)
ISSN 2255-9086 (print)
December 2018, vol. 21, pp. 49–53
doi: 10.7250/itms-2018-0007
https://itms-journals.rtu.lv

Security Aspects of Information Structures in the Information Warfare Context

Pēteris Grabusts
Rezekne Academy of Technologies, Rezekne, Latvia

***Abstract* – In the modern sense, the concept of information warfare includes the use and management of information and communication technologies to achieve a competitive advantage compared to the opponent. Information warfare is manipulation with information that trusts a goal without an objective understanding, so that the goal is to take decisions against its own interests in the interests of the opponents. Information structures are considered to be systems that produce and process various types of information, provide the storage of information and access to users. Such information structures may include neural networks, adaptive learning systems, etc. They must be prepared to train, respond to threats and ensure the safety of their existence, which is very topical during modern information warfare. This analytical article will cover more theoretical aspects related to the security of information systems from the system theory point of view. Knowledge base of the information structure can be a neural network, in which training should be provided from external threats. The author considers artificial neural networks to be one of the potential threats in the context of information warfare.**

***Keywords* – artificial neural networks, cyberwar, information structures, information warfare, neural networks.**

I. Introduction

American researcher Harold Dwight Lasswell [1] can be called the leading theorist of the information warfare of the first half of the 20th century. He actively used the methods of social psychology, psychoanalysis and psychiatry in the study of political behaviour and propaganda, revealing the role of mass media during the information warfare of various states of the world for power. He singled out four main functions of mass media:

- observing the world (collecting and spreading the information);
- "editing" (selecting and commenting the information);
- public opinion formation;
- the spread of culture.

Obviously, all these functions are active components of information warfare.

The strategy of waging the information warfare through impact on public opinion presupposes awareness of the moods of all social, confessional and ethnic groups, awareness of the real state of things. Hence, on the one hand, there is informational-psychological impact through all possible channels, and on the other – a thorough study of public opinion, i.e., the identification of a reaction – the relationship of the elite and the population to informational-psychological influences, so that it is possible to make adjustments to the parameters of the impact.

II. The Evolution of the Concept "Information Warfare"

The term "information warfare", as the 4th generation war, appeared in the late 1980s and became popular very quickly. Thus, in the early 1990s, the first theoretical, and later, practical works appeared, where various definitions of the "information warfare" were given.

Currently, the term "cyberwar" that is often endowed with the content and meanings attributed to "information warfare" is also actively used.

The first profound definition of the term "information warfare" was given in the report of the American RAND Corporation "Strategic Information Warfare: a New Face of War" in 1996 [2]. According to it, "Information warfare is a war in the information space" i.e., to the existing at that time 3 military spaces (land, naval and air), a new information space was added.

Subsequently, in the cooperative document developed by headquarters of "Joint Doctrine for Information Operations" in 1998 [3] the definition of the information warfare was given – "information operations – a conflict in which crucially important and strategically important resource is information that is to be developed or destructed". This is a multi-dimensional concept, which is only one of the aspects, the dimension of which is purely military. The term "information operations" makes it possible to more accurately, than the traditional term "information warfare", investigate the place and role of information confrontation as components of global confrontations.

There are many other definitions, both official and not official. According to the work "Information Warfare and Security" by D.E. Denning [4], "Information war is a set of operations aimed at or exploiting information resources".

The most profound definition of information warfare was suggested by the American theorist M. Libicki in his work "What Is Information Warfare?" dated 1995, where he singled out 7 types of information warfare [5]:

- military confrontation for monopolizing command-control functions;
- confrontation of intelligence service and counterintelligence;
- confrontation in the electronic sphere;
- psychological operations;
- organised spontaneous hacker attacks on information systems;
- informational-economic wars for controlling the trade of information products and monopolizing the

information that is necessary to overcome the competitors;
- cybernetic wars in virtual space.

In a more modern interpretation, the information operation (Info Ops) is understood as an integrated use of the possibilities of electronic weapons, computer network operations (CNO), psychological operations (PSYOP), operations with military disinformation and disorganisation and security operations (OPSEC) to use the possibilities of influencing the human consciousness with the aim of destroying, corrupting, or in general intercepting the influence on the decision-making processes of the enemy, while protecting one's own (decision) [6] (see Fig. 1).

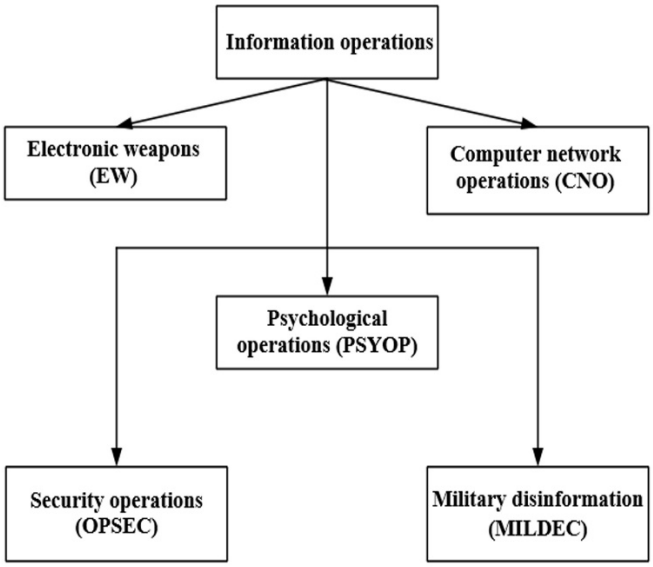

Fig. 1. Components of information operations.

III. Types and Characteristics of Information Warfare

Information warfare can be used among military and among civilian population. One separate type of information warfare or a set of events can be used for this purpose. The types of information confrontation include:

1. information warfare on the internet – different and often contradictory information is offered, used to disorient the enemy;
2. psychological operations – selection and offering of the information, which seems like a counterargument to the moods existing in society;
3. disinformation is the promotion of false information with the purpose to direct the enemy on the wrong track;
4. destruction is the physical destruction or blockage of electronic systems important to the enemy;
5. security steps – strengthening the protection of the resources in order to save plans and intentions;
6. direct information attacks – a mixture of false and truthful information.

Information warfare can be waged both within the state and between different countries. The effectiveness of information warfare depends on well-organized agitation based on the feelings and desires of members of society.

The goal of information warfare is to impact society through information. The signs of information warfare include:

- restriction of access to certain information: blocking web resources, television programmes, printed publications;
- creating a negative background on specific issues (fake news etc.);
- the infiltration of information into various spheres of society.

IV. Means of Implementation of Information Attacks

Today there are many ways and methods of information warfare. The author singles out software and media.

Software can be classified according to the tasks performed with their help on the means of information collection, means of distortion and destruction of information and means of influence on the functioning of information systems. Some means can be universal and used for distorting or destroying information, and for influencing the functioning of information systems.

The main methods and techniques of using information weapons can be as follows:

- damage to separate elements of the information infrastructure;
- destruction or damage of information, programme resources of the enemy, overcoming protection systems, introduction of viruses, programme bookmarks and logical bombs;
- the impact on the software and databases of information systems and management systems with the aim of distorting or modifying them;
- seizure of media channels with the aim of spreading disinformation, rumours, demonstrating strength and bringing their demands;
- destruction and suppression of links, artificial overloading of switching nodes;
- impact on computer equipment to disable it.

Typically, the media uses various methods of negative information impact:

- use of compromising information in order to create a negative image of the politician;
- special reduction of selected negative facts about this or that phenomenon, creation of numerous special TV programmes and headings in newspapers.

First, a "plurality of opinions" is constructed. Then a more definite opinion about the event is expressed, providing it with "expected results".

At the third stage – in debates and disputes – unnecessary arguments are discarded in favour of one definite and unchanging decision.

The fourth stage is the introduction of the fact or evaluation of the event, which is presented as "the prevailing conviction" in the form of "people's tendency to unanimity" in the interests of ordinary citizens.

The policy of targeted influence on public opinion presupposes awareness of the moods of the broad masses of people realising the real situation. Hence, on the one hand, there is information and psychological impact on all possible channels, and on the other – a thorough study of public opinion.

V. Trends and Development of Information Warfare

Information warfare accompanies the history of all mankind. Propaganda can be admitted as the first element of information warfare.

The French sociologist J. Ellul suggested distinguishing between vertical and horizontal propaganda. Vertical is a classic variant of propaganda – an information flow from the top down with a passive audience response [7].

Horizontal propaganda is realized in the group, but does not come from above. In this situation all participants are equal.

Today's business actively uses the methods of propaganda under other names – public relations (PR) and advertising.

J. Stein in 1995 published the study "Information Warfare" [8], where he emphasises that information warfare deals with ideas. Concerning more specific goals, he states the following: "The target of information warfare, then, is the human mind, especially those minds that make the key decisions of war or peace and, from the military perspective, those minds that make the key decisions on if, when, and how to employ the assets and capabilities embedded in their strategic structures".

In his book "War and Anti-war", A. Toffler gives examples of what is most often used to influence others [9]:

- accusations of atrocities;
- bid hyperbolization;
- demonization and dehumanization of the opponent;
- polarization;
- divine sanctions;
- meta-propaganda, which discredits the propaganda of the other side.

J. Arquilla [10] has formulated the rule: only the network structure can effectively work against the network structure; therefore, the hierarchical structures that belong to the state will always lose to the network structures. He has formulated the following three rules of this struggle:

- hierarchies find it difficult to fight networks;
- you need networks to fight with networks;
- those who master the first network forms will have significant advantages.

The current situation of information operations can be seen in a series of publications [2], [11].

VI. Informational Warfare – Influence on Information Structures

The information is tried to be saved in such a way that it can be easily navigated with a possibility of quickly finding the needed information element.

Therefore, the information is structured, i.e., it is written in a definite scheme.

Information structure is now the most common term for those aspects of a sentence meaning that have to do with the way in which the hearer integrates the information into already existing information. To put it more simply, information structure is the domain of language structure and language study that is concerned with notions such as topic, comment, presupposition, and focus [12].

An information system is a system that performs obtaining input data, processing the data, the output of a result or a change in its external state.

Information warfare between two information systems is the open and hidden targeted informational impacts of two systems on each other with the aim of obtaining a certain prize.

Information impact is implemented by using information weapons, i.e., such means, which allow carrying out the conceived actions with the transmitted, processed, created, destroyed and perceived information.

Information weapons are directly related to algorithms. Therefore, it is possible to refer any system to an information system – an information warfare object, if it is capable of processing an algorithm based on input data.

One of the key issues that leads to the insolvability of the problem of winning information warfare is the following: "Is the information system capable of determining that information warfare has been launched against it?".

The author [12] considers that the problem of constructing an algorithm for determining the beginning of information warfare, in general, is algorithmically unsolvable (see Fig. 2).

The scheme above does not represent all possible approaches and techniques to the organisation and conduct of operations on information impact.

It can be concluded that information weapons are primarily an algorithm. To use the information weapon means to select the input data for the system with the aim to activate certain algorithms in it, and in case of their absence, to activate algorithms for generating the necessary algorithms.

The following information will concern the information structures – training systems – in the simplified assumption it could be artificial neural network (ANN) and social networks. It is assumed that the information structure is a knowledge carrier and knowledge of the information system is expressed through its structure. Then, to evaluate the amount of information perceived by the system, it is logical to use such a notion as the degree of structure modification by input data. For example, the weight coefficients of neural links have changed – this is one information, but when elements have been cancelled or appeared – other information.

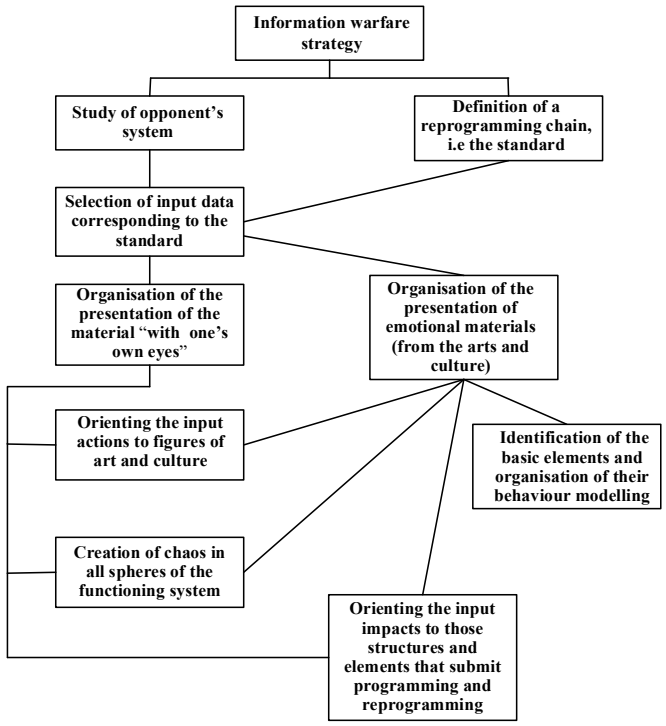

Fig. 2. Typical information warfare strategy.

It can be stated that the information structure is resistant against external effects, if the number of its elements does not undergo sharp fluctuations from these effects.

What structure should a system have in order to prevent the number of its elements from experiencing sharp fluctuations? This is structure A, in which there are several groups of elements that are closely interconnected, but the relationships between groups are very unstable, for example, (see. Fig. 3) [12]:

Structure A: 1 – (2, 3, 4), 2 – (1, 3, 4), 3 – (1, 2, 4), 4 – (1, 2, 3, 5), 5– (4, 6, 7), 6 – (5, 7), 7 – (5, 6).

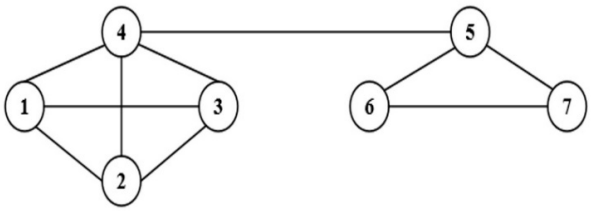

Fig. 3. An example of stable information structure A.

In structure A, it is enough to destroy an element with number 4 and the number of elements of the system is reduced by two times. Clearly, this structure is not stable (any structure is unstable, in which there are single elements carrying out a bunch of group elements).

The structure of the system determines not only the resistance to external and internal effects, not only the time of reaction to this or that threat, but even such parameters as information security, the tendency to corruption, the level of complexity of the tasks solved by the organisation.

Conversely, the most stable system can be considered a system where the structure has the maximum connections, each element is connected to each, i.e., each element is basic.

ANN, in general, cannot be considered stable information structures. It is connected with various training algorithms that work mostly on "black box" principle, which can make them vulnerable to various external threats.

Artificial neural networks are a popular approach in the field of machine learning and perception. Traditionally, they attribute the properties of self-learning, self-organisation, and the ability to process figurative information in opposition to conventional algorithms, which are also traditionally considered to be hard-coded, untraceable, and intended for processing symbolic information.

The more complex the network, the more parameters it has, the more data is required for its training. Usually we do not understand the connection between the trained neural network and the simulated phenomenon. It is not clear in detail why it works and we cannot predict in what cases it can fail.

The issue of limiting AI has been raised in recent years [13], [14]. An AI box is a hypothetical isolated computer system where a possibly dangerous AI is kept constrained in a "virtual prison" and not allowed to manipulate events in the external world. Such a box would be restricted to minimalist communication channels. Unfortunately, even if the box is well-designed, a sufficiently intelligent AI may nevertheless be able to persuade or trick its human keepers into releasing it, or otherwise be able to "hack" its way out of the box [13].

The author presents his viewpoint of AI as the protection information structure in the context of information warfare.

In the context of information warfare, against the certain AI system (ANN or social network based on it), a certain threshold is set up which, apparently, should be calculated by some methodology, taking into account various activities within the framework of the system (fake news, social surveys etc.). The importance of the problem should be taken into account by the system's developer (corporation) and, in case of a critical situation, by the government.

In any case, the system should have an inbuilt mechanism that could be called a trigger, which should respond to an extraordinary intrusion into its structure in the context of the information warfare. At the same time, the system is learning, re-learning and self-learning.

In case the information warfare attacks against the information structures, the trigger responds and there could be four possible situations (see Fig. 4):

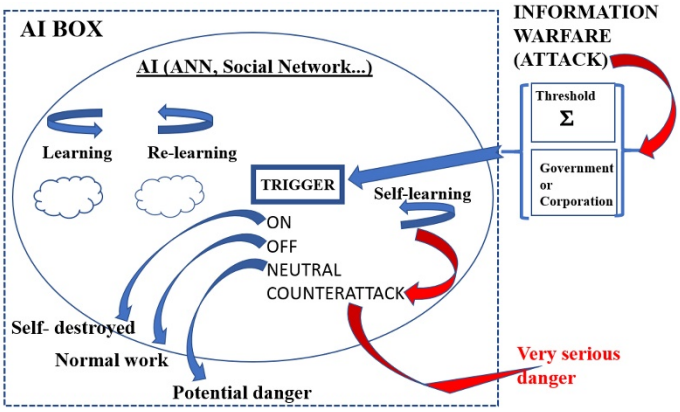

Fig. 4. Potential reaction structure in case of information warfare attack.

1. trigger "on" – the self-destroyed mechanism is launched – the network activity is paralyzed, links are destroyed. The AI box protocol is interrupted;
2. trigger "off" – the attack is treated as false alarms and the system continues to work in the previous mode under the AI box protocol;
3. trigger "neutral" – the attack is treated as an unknown alert and the system continues to work in the previous mode under the AI box protocol, but by intensifying the analysis of the causes of the attack and trying to identify and prevent future threats;
4. trigger "counterattack" – self-learning allows the system to exit the AI box protocol framework and the effects are not predictable.

VII. Conclusion

Information warfare is a war of technologies; it is a war in which the structures of systems, as bearers of knowledge, interfere. It is necessary to talk about methods of information warfare because the understanding of the techniques of information warfare allows one to transfer it from the category of hidden threats into evident ones, with which one can deal.

Consequences of information warfare:

- death and emigration of part of the population;
- destruction of industry;
- loss of territory;
- political dependence on the winner;
- the destruction (sharp reduction) of the army or the ban on one's own army;
- export of the most prospective and high technologies from the country.

The research presents a description of a potential counteraction against the threats of information warfare against information systems (AI based on neural networks).

References

[1] H. Lasswell, "The Structure and Function of Communication in Society," in *The Communication of Ideas*, L. Bryson, Ed. Institute for Religious and Social Studies, 1948, p. 117.

[2] R. C. Molander, A. Riddile and P. A. Wilson, "*Strategic Information Warfare: a New Face of War,*" RAND Corporation, 1996. [Online]. Available: https://www.rand.org/pubs/monograph_reports/MR661.html [Accessed: September 29, 2018].

[3] "Joint Publication 3-13/Information Operations," Oct. 9, 1998. [Online]. Available: http://www.c4i.org/jp3_13.pdf. [Accessed: September 29, 2018].

[4] D. E. Denning, *Information Warfare and Security*. Addison-Wesley, 1999.

[5] M. C. Libicki, *What Is Information Warfare?*, National Defense University, Institute for National Strategic Studies, 1995.

[6] "Information Operation Roadmap," Oct. 30, 2003. [Online]. Available: http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/27_01_06_psyops.pdf. [Accessed: September 29, 2018].

[7] J. Ellul, *Propaganda: The Formation of Men's Attitudes*, Vintage Books, New York, 1965.

[8] G. J. Stein, "Information Warfare," 1995. [Online]. Available: http://www.iwar.org.uk/iwar/resources/airchronicles/stein.htm. [Accessed: September 29, 2018].

[9] A. Toffler, *War and anti-war. Survival at the dawn of the 21st century*, Little Brown & Co., 1993.

[10] J. Arquilla and D. Ronfeldt, "*The Advent of Netwar*, "RAND Corporation, 2001, [Online]. Available: https://www.rand.org/pubs/monograph_reports/MR1382.html [Accessed: September 29, 2018].

[11] D. Ventre, *Information Warfare*, 2nd Edition, Wiley, 2016. https://doi.org/10.1002/9781119004721

[12] S. P. Rastorguev, *Information Warfare*, M: Radio and Communication, 1998 (in Russian).

[13] D. Chalmers, "The Singularity: A Philosophical Analysis," *Journal of Consciousness Studies*, vol.17, no. 7–65, Jan. 2010.

[14] R. V. Yampolskiy, "What to Do with Singularity Paradox?," in *Philosophy and Theory of Artificial Intelligence*, vol. 5, V. C. Muller Ed. Berlin, Germany: Springer-Verlag, 2013, pp. 397–413. https://doi.org/10.1007/978-3-642-31674-6_30

Pēteris Grabusts received his *Dr. sc. ing.* degree in Information Technology from Riga Technical University in 2006. Since 1996, he has been working at Rezekne Academy of Technologies. Since 2014, he has been a Professor at the Engineering Faculty. His research interests include data mining technologies, neural networks and clustering methods. His current research interests include ontologies.
E-mail: peteris.grabusts@rta.lv