Informational Warfare – Influence on Informational Structures

Peter Grabusts
Engineering Faculty
Rezekne Academy of Technologies
Rezekne, Latvia
peteris.grabusts@rta.lv

Aleksejs Zorins
Engineering Faculty
Rezekne Academy of Technologies
Rezekne, Latvia
aleksejs.zorins@rta.lv

Artis Teilans
Engineering Faculty
Rezekne Academy of Technologies
Rezekne, Latvia
artis.teilans@rta.lv

***Abstract*— The concept of information warfare encompasses the use of information and communication technologies to gain an advantage over a potential opponent. The information warfare is the manipulation with the information that trusts the goal, so that the goal should make decisions about its interests in the interests of opponents. Information structures are treated as systems that process different types of information, provide storage and access to users. Such structures may enclose neural networks, self-learning systems etc. They need to be ready to learn, respond to threats and ensure their safety, which is topical in today's information warfare. This paper will address aspects related to the security of information systems from a system theory point of view. The knowledge base of information structures can be elements of artificial intelligence, which security must be protected against various threats. The authors considers artificial neural networks to be one of the potential threats in the context of information warfare.**

Keywords*— *artificial neural networks, information structures, information warfare, neural networks.

I. Introduction

The information warfare have always existed - between individuals, groups, races, religions, states, cultures, civilizations. It is always the forerunner and driving force of different wars.

H. Lasswell [1] can be named the information warfare theorist of the first half of the 20th century. He actively used the methods of social psychology, psychoanalysis in the study of political behavior and propaganda, identifying the role of mass communications during information warfare of various states of the world for power. He outlined four main media functions:

- collection and dissemination of information;
- selection and commenting of information;
- formation of public opinion;
- spread of culture.

Obviously, all these components are active parts of the information warfare.

The strategy of waging the information warfare by targeting public opinion presupposes awareness of the moods of all social and ethnic groups, awareness of the real state of things. Consequently, on the one hand, informational and psychological effect through all possible channels, and on the other hand, a meticulous study of public opinion, that is, the revealing of the reaction - the relationship of the elite and the population to informational and psychological impacts, so that you can make adjustments to the impact parameters.

In order for the public to survive in the condition of information warfare, it needs an understanding of the information structures and their ability to counteract the effects of the information warfare. They try to store information so that it can be easily oriented in it, that is, to quickly find the necessary information element. Therefore, information is structured, that is, recorded in a specific pattern.

Information structure is now the most common term for those aspects of a sentence's meaning that have to do with the way in which the hearer integrates the information into already existing information.

An information system is a system that performs: obtaining input data; processing the data; issuing a result or changing its external state. Information warfare between two information systems is open and hidden targeted informational effects of systems on each other in order to obtain a certain gain.

Information impact is realized with the use of information weapons, i.e. such means that allow the planned actions to be realized with the transmitted, processed, created, destroyed and perceived information.

The aim of the work is to study the impact of information warfares on information structures.

II. The essence of the information warfare

The term "information warfare", the 4th generation war, was introduced in the late 80s and became widely used. Then, in the beginning of the 90s, the first theoretical and later practical works were published, where numerous definitions of the "information warfare" were presented.

Print ISSN 1691-5402
Online ISSN 2256-070X
http://dx.doi.org/10.17770/etr2019vol2.4035

Nowadays, the concept “cyber war” is also widely used, which quite often is endued with content and meanings that are assigned to “information warfares”.

The first deep definition of the concept “information warfare” was given in the 1996, in a report of the American RAND corporation “Strategic Information Warfare and the New Face of War” [2]. According to it, “Information warfare is a war in the information space”. At that time 3 military spaces (land, naval and air) existed and a new one - information space - was added.

Afterwards, the headquarters of the “Joint Doctrine for Information Operations”, 1998 [3], worked out the joint document where a definition of “information warfare” as “information operations - a conflict in which a critical and strategically important resource is information that must be exploited or destroyed “ was given. It is a multidimensional concept, which represents only one aspect, the dimension of which is mainly military. The concept “information operations” gives a chance, more accurate than the traditional term “information warfare”, investigate the place and role of information confrontation as elements of global confrontations.

There are a lot of other definitions of “information warfare”, both official and non-official. D. Denning [4] in his work “Information Warfare and Security” noted: “Information warfare is a number of operations that have the purpose to gain or operate the information resources”. Another researcher, G. Stein in his work “Information Warfare” [5] asserted: “Information war - is the use of information to achieve our national goals”.

The most profound definition of “information war” was offered by the American theorist M. Libicki in his work “What Is Information Warfare?” dated 1995, where he distinguished 7 types of information warfares [6]:

- 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.

Information warfare can be used among the military and among civilians. For this purpose one of the types of information warfare or a set of actions can be used. The following types of information standoff can be defined:

- Information warfare on the Internet - different and often conflicting pieces of information are offered, which are used to confuse the enemy.
- Psychological operations - screening and supplying of such information, which sounds like a counter-argument on the mood that exists in society.
- Misinformation - stimulation of false information with a purpose to guide the enemy side to the wrong way.
- Destruction - the physical destruction or blocking of electronic systems that are important to the opponent.
- Security measures – intensification of the security of the resources with a purpose to save plans and intentions.
- Direct information attacks - combination of false and truthful information.

G. Stein issued the study “Information Warfare” [5], where he highlighted that information warfare operates with ideas. With regard to more specific aims, he claims the following: “The goal of the information warfare is the human mind, especially the one that makes the key decisions of war and peace, and the one that makes the key decisions about where, when and how to use the potential and opportunities that appear in their strategic structures”.

In his book “War and Anti-war”, A. Toffler [7] gives some examples of what is most often used to make an impact on others:

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

Presently, there are several means and methods of information warfare [8], [9]. The authors differentiates software and media.

Software can be categorized according to the tasks performed with their help. The following can be distinguished: information collecting tools, distorting and destroying information tools and tools influencing on functioning of information systems. Some tools can be universal and used to distort or destroy information, and to impact the functioning of information systems.

The main techniques and methods of applying information weapons are following:

- damage to particular elements of the information infrastructure;
- destroying or damaging of enemy information and software resources, overcoming protection systems, implantation of viruses and logic bombs;
- influence on software and databases of information systems and control systems with the purpose of their distortion or modification;

- taking over media channels with a purpose to spread misinformation, rumors, demonstrate power and bring in their demands;
- destruction and repression of communication lines, simulated overloading of switching nodes;
- influence on computer equipment with a purpose to disable it.

III. Information structures

Information weapon is directly related to the algorithms. Therefore, it is possible to call any system an information system – the object of information warfare – if it is capable of processing an algorithm according to the input data.

One of the crucial questions that shows the undecidability of the problem of winning an information warfare is the following: “Is the information system able to determine that information warfare has been launched against it?”

Why is it important to protect the information structure from information? It is vital because any information entering the system necessarily changes the system. Focusing informational impact can lead to irreversible changes and self-destruction.

Therefore, information warfare is nothing but explicit and hidden targeted informational actions of systems on each other with a purpose to get a certain win. Practising of information weapons means the supplying to the input of the information self-learning system such a sequence of input data, which activates certain algorithms in the system.

The conclusion is, that information weapon is, first of all, an algorithm. Applying an information weapon means choosing the input data for the system in such a way that it could activate certain algorithms in the system, and in the case of the absence of necessary ones activate the algorithms for generating the necessary algorithms.

Further it goes about information structures - learning systems - in the simplest assumption it could be an artificial neural network (ANN) and social networks. It is assumed that the information structure is the bearer of knowledge and knowledge of the information system is expressed through its structure. Then, to estimate the amount of information received by the system, it could be logical to use such a concept as the degree of structure modification by the input data.

It can be said that the information structure is stable against external influences if the number of its elements does not have sharp fluctuations from these influences.

What structure should the system have so that the number of its elements do not experience sharp fluctuations? This is a structure in which there are several groups of elements that are closely related to each other, but the connections between the groups are very unstable, for example: 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).

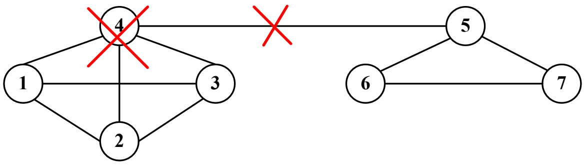

Fig. 1. An example of stable information structure.

In structure A, it is enough to destroy the element with number 4 and, as a consequence, the number of elements of the system will be reduced by half. Clear, that this structure is not stable (unstable is any structure in which there are single elements that carry out a bundle of groups of elements) [10].

Conversely, the most stable system can be considered a system in the structure of which there is the maximum number of connections — each is connected to each, i.e. each element is basic.

Different information systems may contain various information structures that can be described in an analytical or graphical way that describes the knowledge base of structures. It is necessary to formulate task classes necessary for describing information structures [10]:

- Assessment of information structure capabilities.
- Assessing the form of information structure, which is maximum resistant to external threats at the moment.
- Determining the minimum configuration of an information structure that is resistant to threats.
- Predicting the effect of potential changes in information structures.
- Attempts to predict a factor that could affect the stability of the structure and, as a result, it could be modified or collapse.

For example, what should be the impact strategy on the structure shown in Figure 2, so that the realization of the external impact could lead the system to destruction (structure A: 1 – (2, 3), 2 – (1, 4, 5), 3 – (1, 6, 7), 4 – (2), 5– (2), 6 – (3), 7 – (3))?

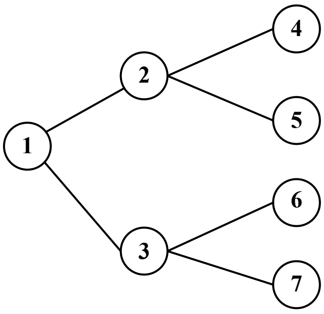

Fig. 2. An example of information structure.

IV. Risk of information structures

In general, artificial neural networks cannot be considered as stable information structures. It is related to various learning algorithms, which mostly work on the “black box principle”, which can make them unprotected to various external threats.

A popular approach in machine learning and perception is artificial neural network. Traditionally, they are assigned to the properties of self-learning, self-organization, ability to process figurative information as opposed to the usual algorithms, which are also traditionally considered to be rigidly defined, untrained, and intended for processing symbolic information.

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

In recent years, the issue of restricting artificial intelligence (AI) has become topical [11], [12].

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 [11].

The authors offers his own viewpoint of AI as a protection of information structures during information warfare [13].

In terms of information warfare, a certain threshold is set against an AI system (ANN or social network based on it), which, apparently, should be counted according to some methods taking into account certain activities within the system (fake news, social polls, etc.). The importance of the problem must be recognized by the corporation and, in case of a critical situation, the government.

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

If, in case of an information warfare attack against the information structures the trigger had to respond, five situations would be possible (see Fig. 3):

- trigger "ON" – the self-destroyed mechanism is launched – the network activity is paralyzed, links are destroyed. The AI box protocol is interrupted;
- trigger "OFF" – the attack is treated as false alarms and the system continues to work in the previous mode under the AI box protocol;
- 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;
- trigger "COUNTERATTACK" – self-learning allows the system to exit the AI box protocol framework and the effects are not predictable.
- trigger "UNKNOWN" – the effects are not predictable.

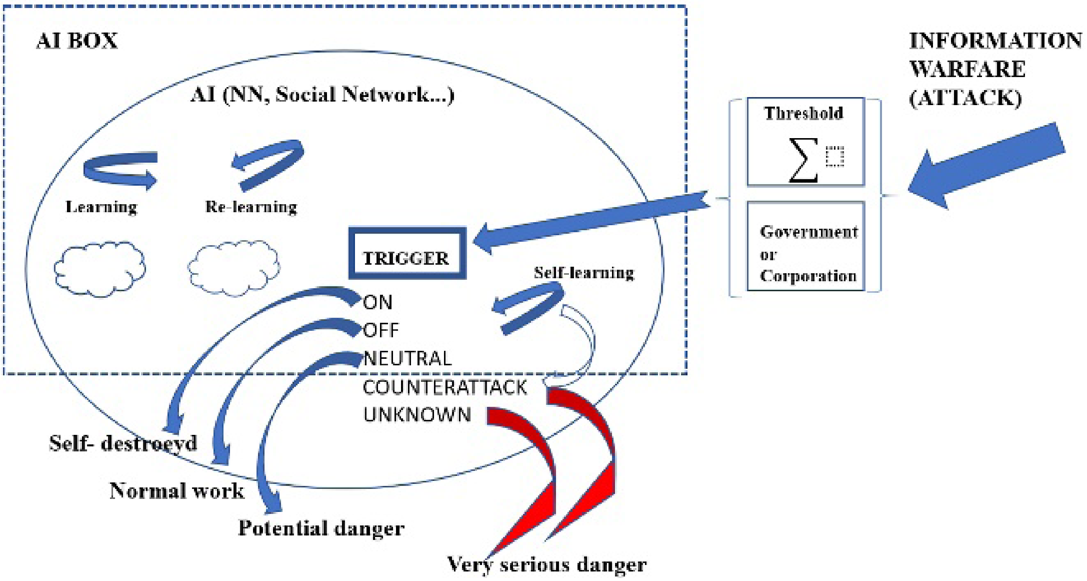

Fig. 3. Potential counteraction structure in case of information warfare attack.

V. Conclusions

Information warfare in essence is a war of technology. It is a war in which exactly the structures of systems, as knowledge holders, interfere. It is necessary to talk about the methods of information warfare because an understanding of the techniques of information warfare makes it possible to transfer it from the category of hidden threats into explicit ones that can be dealt with.

Consequences of information warfare:

- death or emigration of part of the population;
- the destruction of industry;
- loss of part of the territory;
- political dependence on the winner;

- the destruction (sharp reduction) of the army or a ban on its own army;
- export of the most promising and knowledge-intensive technologies from the country.

Information warfare is nothing but explicit and hidden targeted informational actions of systems on each other with a purpose to get a certain win. Practising of information weapons means the supplying to the input of the information self-learning system such a sequence of input data, which activates certain algorithms in the system.

The research presents a description of a potential counteraction against the threats of information warfare against information systems (AI based on artificial 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: March 10, 2019].

[3] “Joint Publication 3-13/Information Operations,” Oct. 9, 1998. [Online]. Available: http://www.c4i.org/jp3_13.pdf. [Accessed: March 10, 2019].

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

[5] G. J. Stein, “Information Warfare,” 1995. [Online]. Available: http://www.iwar.org.uk/iwar/resources/airchronicles/stein.htm[-Accessed: March 10, 2019].

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

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

[8] A.Nestoras, “Political Warfare: Competition in the Cyber Era,” IEEE International Conference on Big Data, Big Data 2018, 10-13 December 2018, https://doi.org/10.1109/BigData.2018.8622490.

[9] V.Duddu, “A survey of adversarial machine learning in cyber warfare,” Defense science journal, Volume 68, Issue 4, July 2018, Pages 356-366, doi: 10.14429/dsj.68.12731

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

[11] D. Chalmers, “The Singularity: A Philosophical Analysis,” Journal of Consciousness Studies, vol.17, no. 7-65, Jan. 2010.

[12] 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

[13] P.Grabusts, “Ensuring the security of information structures in today’s environment,” 59th International Scientific Conference on Information Technology and Management Science of Riga Technical University, ITMS 2018 – Proceedings, 29 November 2018, https://doi.org/10.1109/ITMS.2018.8552976.