Information structures in the framework of information warfare – ontology approach

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

***Abstract*—The concept of information warfare involves the use of information and communication technology to achieve an advantage over a potential enemy. The goal is to take decisions against their interests in the interests of their enemies. Information structures are treated as systems that process various types of information, provide its storage and access to users. Such structures may include neural networks, self-learning systems, etc. They must be prepared to train, respond to threats and ensure the safety of their existence, which is topical during the modern information warfare. In this paper, the theoretical aspects related to the security of information systems from the point of view of the system theory and ontology approach will be considered. Knowledge base for information structures can be elements of artificial intelligence, which must be secured against external threats. Ontologies have gained increasing interest in the computer science community and their benefits are now recognized for different applications.**

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

I. Introduction

The information warfare has always existed - between separate individuals, groups, races, religions, countries, cultures, civilizations. It is always the forerunner and driver of various wars. H. Lasswell [1] can be called 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 media in the course of information warfare of various states in the world for power. He identified four main functions of mass media:

- Collecting and spreading of information.
- Selection and commenting of information.
- Public opinion formation.
- Spread of culture.

It is obvious that all these functions are active components of the information warfare.

The strategy of conducting information warfare by purposeful influence on public opinion presupposes knowing the moods of all social and ethnic groups, knowing the real state of things. Hence, on the one hand, informational and psychological impact through all possible channels, and on the other hand, a thorough study of public opinion, that is, the identification of the reaction — the relationship of the elite and the population to informational and psychological influences, in order to make adjustments to the impact parameters.

In order for the public to survive in the context of information warfare, it needs to understand the information structures and their ability to oppose the impact of the information warfare.

The information is tried to be stored so that it can be easily navigated, that is to quickly find the desired information element. Therefore, the information is structured, that is, it is written in a definite scheme. Information structure (IS) 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 provides: receiving input data; processing of the data; giving out a result or changing its external state.

An information warfare between two information systems is an open and hidden purposeful information influence of systems on one another with the purpose of getting a certain win.

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

The aim of the work is to explore the possibilities of ontologies to describe the information structures in case of danger.

II. The Concept of Information Warfare

The term “information warfare”, as the 4th generation war, appeared in the late 80s and very quickly gained popularity. So in the beginning of the 90s, the first theoretical and later practical works appeared, where various definitions of the “information warfare” were given.

Nowadays, the term “cyber war” is used in parallel, which is often endowed with content and meanings attributed to “information warfare”.

The first profound definition of the term “information warfare” was given in the 1996 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”. That is, a new information space is added to the 3 military spaces (land, naval and air) existing at that time.

Subsequently, in the joint document developed by the headquarters of “Joint Doctrine for Information Operations" [3] the definition of “information warfare”, as information operations - conflict in which critically and strategically important resource is information that is to be mastered or destructed was given. This is a multidimensional concept, which is only one aspect, the measurement of which is purely military. The term “information operations” makes it possible, more precisely than the traditional term “information warfare” explore the place and role of information confrontation as components of global confrontations.

There are many other definitions, both official and nonofficial. According to the work “Information Warfare and Security” D. E. Denning said [4]: “Information warfare is a set of operations that have the aim or to exploit the information resources". But in the work of G. J. Stein "Information Warfare" [5]: "Information warfare - is the use of information to achieve our national goals."

The most profound definition of “information warfare” was proposed by the American theorist M.C. Libitsky in his work “What Is Information Warfare?” dated 1995, where he identified 7 types of information wars [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. One of the types of information warfare or a set of activities can be used for this purpose. The types of information opposition include:

- Information warfare on the Internet - different and often contradictory information is offered, which is used to confuse the enemy.
- Psychological operations - the selection and delivering of such information, which sounds like a counter-argument on the mood that exists in society.
- Disinformation - the promotion of false information in order to direct the opponent side on the wrong track.
- Destruction - the physical destruction or blocking of electronic systems that are important to the enemy.
- Security measures - strengthening the protection of the resources in order to preserve plans and intentions.
- Direct information attacks - confusion of false and truthful information.

Information warfare can be carried out both within the state and between different countries. The effectiveness of information warfare depends on well-composed campaigning, based on the feelings and desires of members of society.

The essence of the information warfare is to influence the society through information. The signs of information warfare include:

- Restriction of access to certain information: the closure of web resources, television programs.
- Creating a negative background on specific issues (fake news).
- Spreading of forced information in various spheres of society.

III. Tendences of Information Warfare

Information warfares follow the entire history of mankind. Propaganda can be considered the first version of the information warfare. French sociologist J. Ellul [7] offered to differentiate vertical and horizontal propaganda. Vertical - this is a classic version of propaganda - information flows from top to bottom with a passive response from the audience.

Horizontal propaganda is realized in the group, and does not come from above. In this situation, all participants are equal. Today’s business actively uses propaganda impact methods under other names - public relations and advertising.

G. J. Stein publishes the study “Information Warfare” [5], where he emphasizes that information warfare deals with ideas. Regarding to more specific aims, he states 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 apply the potential and opportunities that are in their strategic structures”.

In his book “War and anti-war", A. Toffler gives examples of what is most often used to influence others [8]:

- 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 [9] has formulated the rule: only the network structure can work effectively against the network structure, therefore hierarchical structures that belong to the state will always lose to the network ones. Arquilla has formulated the following three rules for this fight:

- 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.

Today, there are many ways and methods of information warfare. The author distinguishes software and media.

Software means can be classified according to the tasks performed with their help on means collecting information, means of distorting and destroying information, and means of influencing the functioning of information systems. Some means can be universal and used both to distort or destroy information, and to influence the functioning of information systems.

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

- Damage to individual elements of the information infrastructure.
- The destruction or damage to the information and software resources of the opponent, overcoming protection systems, the introduction of viruses, trojans and logic bombs.
- Impact on software and databases of information systems and control systems with the aim to distort or modify them.
- Capturing media channels in order to spread disinformation, rumors, demonstrate power and bring their demands.
- Destruction and suppression of communication lines, artificial overloading of switching nodes.
- Impact on computer equipment in order to disable them.

The policy of purposeful influence on public opinion presupposes knowing the mood of the broad masses of the people, knowing the real state of things. From here, on the one hand, informational and psychological impact through all possible channels, and on the other - a thorough study of public opinion.

IV. Influence of Information Warfare on Information Structures

The information weapons have a direct relation to the algorithms [10]. Therefore, any system capable of processing the given algorithm by input data can be called an information system-the object of an information warfare.

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

Why is it necessary to protect the information structure from information? Because any information entering the system inevitably changes the system. Purposeful information impact can lead to irreversible changes and self-destruction [10].

Therefore, information warfare is nothing but obvious and hidden targeted informational effects of systems on each other in order to get a certain gain.

The use of information weapons means the supply to the input of the information self-learning system of such a sequence of input data that activates certain algorithms in the system.

It can be concluded, that information weapon primarily is an algorithm. To use an information weapon is to select the input data for the system in such a way that certain algorithms are activated in it, and in the case of their absence, activate the algorithms for generating the necessary algorithms [10].

Further, we talk about information structures - training systems - in the simplified assumption it could be artifical neural network (ANN) and social networks. It is assumed that an information structure is a knowledge carrier and knowledge of an 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 concept as the degree of structure modification by the input data.

It can be said that the information structure is resistant to external influences if the number of its elements does not experience sharp fluctuations from these influences.

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

Artificial neural networks are considered to be a popular approach to machine learning and perception. Traditionally, they are attributed to the properties of self-learning, self-organizing, having ability to process figurative information in oppose to conventional 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 why it works and we can not predict in which cases it can fail.

The issue of Artificial Intelligence (AI) limiting has been raised in recent years [11], [12]. An AI box is a hypothetical isolated computer system where a possibly dangerous AI is kept constrained in a “virtual prison" and is 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 nev-

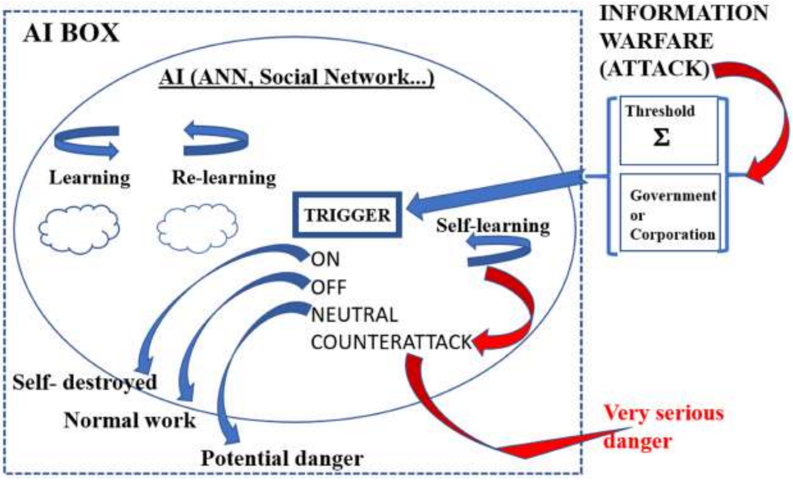

Figure 1. Potential reaction structure in case of information warfare attack

ertheless 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 author presents his viewpoint on AI as the protection of information structures in the context of information warfare. In the context of information warfare against a 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 the various activities within the framework of the system (fake news, social surveys, etc.). The importance of the problem must 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 a developed 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. If, in case of an information warfare attack against the information structures the trigger had to work, four situations would be possible (see Fig. 1):

- 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.

The author did not find a formal description of the IS protection mechanism in the literature available, thus has offered own concept in figure 1.

The paper also looks at considers the decision-making algorithms in trigger management.

V. Ontology Possibilities

In recent years the development of ontologies is formal description of the terms in the domain and the relationships between them that moves from the world of artificial intelligence laboratories to desktops of domain experts [13]. In the World Wide Web ontologies have become common things. Ontologies on the net range from large taxonomies, categorizing Web sites, to categorizations of products sold and their characteristics. In many disciplines nowadays standardized ontologies are being developed that can be used by domain experts to share and annotate information in their fields.

The philosophical term “ontology” is known for a long time, but at the end of the last century, this concept was rethought with regard to knowledge engineering. The classic definition of an ontology in modern information technologies: “An ontology - a formal specification of a conceptualization that takes place in a context of the subject area” [14].

Informally, an ontology is a description of the view of the world in relation to a particular area of interest. This description consists of the terms and rules for the use of these terms, limiting their roles within a specific area. Formally, ontology is a system consisting of a set of concepts and a set of statements about the concepts on the base of which you can build up classes, objects, relations, functions, and theories.

It is accepted that an ontology is a system of concepts of a subject area, which is represented as a set of concepts linked by different relations to determine the field of knowledge. The formal structure of the ontology is an advantage for the quality of the method of knowledge representation.

On a formal level, an ontology is a system consisting of a set of concepts and a set of statements about these concepts, on the base of which we can build classes, objects, relations, functions and theory. The main components of the ontology are classes or concepts, relations, functions, axioms, examples.

There are many and different definitions of ontologies, but the following definition has recently been accepted as generally recognized: “An ontology is a formal explicit specification of a shared conceptualization” [14]. Ontologies are often equated with taxonomic hierarchies of classes. It can be said that the purpose of ontology is to accumulate knowledge in a general and formal way.

Ontologies can be classified in different forms. One of the most popular types of classification is offered by Guarino, who classified types of ontologies according to their level of dependence on a particular task or point of view [15].

- Top-level ontologies - describe the most general concepts that do not depend on the subject areas.
- Domain-ontologies - formal description of the subject area, used to clarify the concepts defined in the meta-ontology and defines a common terminology base of subject area.
- Task ontologies - an ontology that defines a common terminology base, related to a specific task.
- Application ontologies - are often used to describe the outcome of actions performed by the objects of subject area or the problem.

The simplest model of ontology with relations is usually based on a class-subclass relationships. Such models are often called taxonomies - hierarchies of concepts towards investments. Thus, the aim of building an ontology is a representation of knowledge in a particular subject area.

Developing framework Protege OWL tool is used for construct this concept [16].

Protege is an ontology and knowledge base editor. Protege is a tool that enables the construction of domain ontologies, customized data entry forms to enter data. Protege allows the definition of classes, class hierarchies, variables and the relationships between classes and the properties of these relationships.

Protege is a special tool, which is thought to create and edit ontology, but OWL (Web Ontology Language) is a language through which it is possible to define the ontology. OWL ontology may include descriptions of classes, their characteristics and their instances. OWL formal semantics describes how, using these data get information which was not openly described in ontology, but which follows from the data semantics. Protege is a free open-source platform, which contains special tool kit which makes it possible to construct domain models and knowledge-based applications based on ontologies. In Protege environment a number of knowledge-modeling structures and actions that support ontology creation, visualization and editing of different display formats are implemented.

The development of ontologies with Protege begins with the definition and description of the classes hierarchy, after that the instances are assigned of these classes and different type of relationships (properties in Protege) in order to put more meaningful information within the ontology.

The author has previously carried out the research on the ontology-based risk analysis system concept development [17].

The example of the given ontology is of an illustrative nature, showing a possible ontology in case of any threats to information structures.

Unfortunately, the author could not find examples of similar ontologies in the protection of information structures, thus the author provides own solution.

The following class hierarchy is defined (see Fig.2).

The top level of ontology is the *Attack-detection* class. This is an abstract class, which includes all the main classes of the subject area:

- *Government or corporation.*
- *Situation threshold.*

In the class *Situation analysis* the members *Trigger ON*, *Trigger OFF*, *Trigger Counterattack* and *Trigger Neutral* are included.

After rating all risks, the situation is analyzed according to Figure 1. An ontology defined in Figure 2 may be offered to define threats.

An example of a demonstration shows that with a help of Protege an effective ontology description can be created, but it is a sufficiently laborious process. The author plans to continue the work on the further development of information warfare ontology.

VI. Conclusion

Information warfare is a war of technologies; it is a war in which the structures of systems, as carriers of knowledge, collide. 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 and emigration of part of the population.
- Destruction of industry.
- Loss of territory.
- Political dependence on the winner.
- The destruction of the army or the ban on one’s own army.
- Export of the most prospective and high technologies from the country.

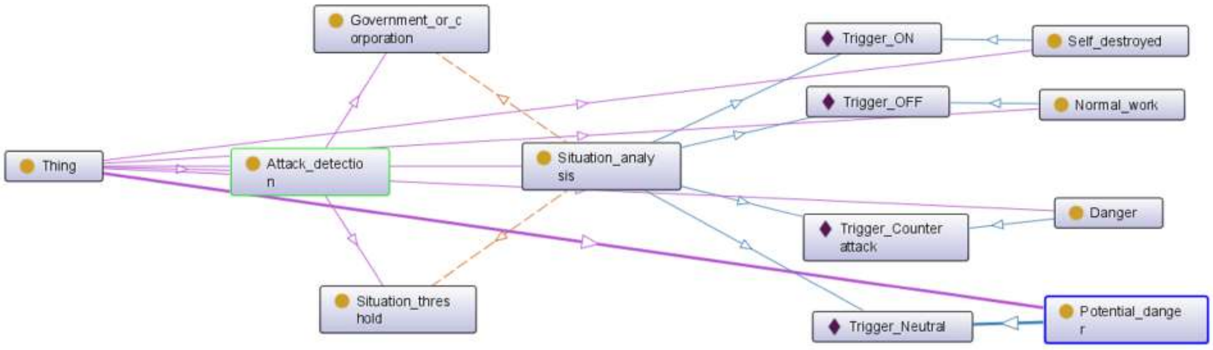

Figure 2. Example of ontology in case of IS threats

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

The creation of ontologies is a promising area of modern research in information processing, including the subject of risk analysis in various fields of application. This article examined the ontology prototype approach for identifying IS threats. The concept of ontology for risk assessment of IS threats was proposed, some classes and subclasses of ontology under development were described. Thus, ontology becomes a system for storing and managing knowledge.

References

[1] H. Lasswell, The Structure and Function of Communication in Society, *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. Available at https://www.rand.org/pubs/monograph_reports/MR661.html (accessed 2018, Nov).

[3] Joint Publication 3-13/Information Operations, Oct. 9, 1998. Available at http://www.c4i.org/jp3_13.pdf (accessed 2018, Nov).

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

[5] G. J. Stein, Information Warfare, 1995. Available at http://www.iwar.org.uk/iwar/resources/airchronicles/stein.htm. (accessed 2018, Nov).

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

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

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

[9] J. Arquilla and D. Ronfeldt, The Advent of Netwar, RAND Corporation, 2001. Available at https://www.rand.org/pubs/monograph_reports/MR1382.html. (accessed 2018, Nov).

[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.

[13] D. Gašević, D. Djurić and V. Devedžić, *Model driven architecture and ontology development*, Springer-Verlag, 2006.

[14] T. R. Gruber, A translation approach to portable ontologies, *Knowledge Acquisition*, 5(2), pp. 199-220, 1993.

[15] N. Guarino, Formal Ontology in Information Systems. *1st International Conference on Formal Ontology in Information Systems*, FOIS, Trento, Italy, IOS Press, pp. 3-15, 1998.

[16] Protege project homepage. Available at: http://protege.stanford.edu/ (Accessed 2018 Nov).

[17] P. Grabusts, O. Uzhga-Rebrov, Ontology-Based Risk Analysis System Concept. *Open semantic technologies for intelligent systems*, OSTIS-2017, Minsk, Belarus, pp. 341-346, 2017.

ИНФОРМАЦИОННЫЕ СТРУКТУРЫ В КОНТЕКСТЕ ИНФОРМАЦИОННЫХ ВОЙН – ИСПОЛЬЗОВАНИЕ ОНТОЛОГИЙ

Грабуст П.С.

Понятие информационной войны подразумевает использование информационных и коммуникационных технологий для достижения преимуществ по сравнению с потенциальным противником. Информационная война – это манипуляция информацией, которой доверяет цель, цель должна принять решения против их интересов в интересах противников. Информационные структуры рассматриваются как системы, обрабатывающие различные виды информации, обеспечивающие ее хранение и доступ к пользователям. Такие структуры могут включать в себя нейронные сети, самообучающиеся системы и т.д. Они должны быть готовыми к обучению, реагировать на угрозы и обеспечивать безопасность их существования, которая является актуальной во время современной информационной войны. В этой работе будут рассмотрены теоретические аспекты, связанные с безопасностью информационных систем с точки зрения теории системы и онтологического подхода. База знаний информационных структур может быть элементами искусственного интеллекта, безопасность которых должна быть обеспечена от внешних угроз. В сфере изучения компьютерных технологий интерес к использованию онтологий возрастает, и их преимущества теперь признаны для разных приложений.

Создание онтологий является перспективным направлением современных исследований по обработке информации, включая тематику анализа рисков в различных областях применения. В данной статье рассматривался подход разработки прототипа онтологии для идентификации угроз ИС. Была предложена концепция онтологии по оценке рисков угроз ИС, описаны некоторые классы и подклассы разрабатываемой онтологии. Таким образом онтология становится системой хранения и управления знаниями.

Received 04.12.18