Conference on Cyber Conflict
Proceedings 2010
C. Czosseck and K. Podins (Eds.)
CCD COE Publications, 2010, Tallinn, Estonia.

KNOWLEDGE BASED FRAMEWORK FOR CYBER WEAPONS AND CONFLICT

Peeter LORENTS and Rain OTTIS

CCD COE, Tallinn, Estonia

Abstract: In recent years there have been a number of international conflicts that have been mirrored by a parallel campaign of hostile actions in cyberspace. This, in turn, has prompted various attempts to analyze the phenomenon and explain the threat to the wider public. Unfortunately, however, the reports and analysis are often confusing and can include rather arbitrary use of various cyber “buzz words“. It follows that there is a need for a formal rigorous model for describing and analyzing cyber conflicts. Formal methods are also necessary for developing artificial intelligence-enabled offensive and defensive systems for cyber conflicts.

In order to provide a remedy for this issue, we propose a formalized framework of key terms in cyber conflict. We begin by revisiting the concepts of knowledge, data and information. Based on that we proceed to define “information system” and “intelligent system”. We provide a formal description for the concept of destroying and falsifying information and explain the concepts of confidentiality, integrity and availability as part of our framework. We then propose definitions for cyber weapons, cyber incidents, cyber attacks, cyber espionage, cyber conflicts and finally, cyberwar.

The framework is based on formal logic and allows for theoretical, experimental or empirical research with mathematically provable results. As such, it can provide a solid backbone for cyber conflict research, which is often based on less rigorous methods.

Keywords: knowledge, data, definitions, cyber weapon, cyber conflict

Disclaimer: This paper is a product of the authors. It does not represent the opinions or official policies of the CCD COE or NATO and is designed to provide an independent position.

INTRODUCTION

Threats from cyberspace differ from most traditional threats, because they are global, often unpredictable and can affect our lives when we least expect them. For example, a political dispute between two countries can unleash a wave of cyber attacks, which take down an international bank, causing discomfort and economic damage in countries unrelated to the conflict. A war on another continent does not pose a threat to the average citizen, but a cyber campaign anywhere in the world can potentially reach us in our homes.

Over the past few years the public perception of the threat from cyber attacks has risen considerably. Therefore, it is important to analyze the phenomenon in a systematic and scientific way. To achieve this, we must either choose or create an applicable terminology and scientific methods, which allow theoretical, experimental and empirical studies with reliable results.

In order to effectively handle events in cyberspace, we (humans) first need to be able to clearly describe these situations and events, and any constraints that apply to them. Based on this we need to derive an appropriate decision for dealing with the situation. The events in cyberspace surpass the human ability to comprehend them, both in terms of the amount of available information, as well as the speed of the changes that take place in cyberspace. One way to manage this problem is to enlist computers to provide decision assistance or even fully automated decisions. This, however, requires that we use a framework that is compatible with the formal logic of the computer. In order to satisfy this requirement, we present a framework (described below) that is based on formal mathematical theories (proof theory, model theory, algebraic systems theory, etc.).

This is the only way to *really* provide a framework which is applicable for both human decision-makers and automated decision support systems, and that is based on a (A) reliable, (B) credible and (C) commonly agreed foundation and that (D) works. The framework can, in turn, be used to:

- adequately explain past, present and potential future cyber events to the public and decision-makers,
- develop means to monitor the situation, assess the threats, as well as provide necessary security and preventive actions,
- create applicable regulations, laws and international treaties.

Unfortunately, there is still no common and general set of exact science and engineering terms that covers the basic concepts of information and communication technology. In other words, there are no commonly agreed terms that would allow formulating arguments and strong proofs of these arguments. For example, the concepts of *knowledge, data* and *information* (not to be confused with the practical measure of information I, which can be found using Hartley's (1928) formula $I=\log_a m^n$).

In this work we focus on understanding terms that are related to information, operating with information and the problems associated with information, including confidentiality, availability and integrity. We finish with the concepts of cyber weapon, cyber incident, cyber attack, cyber espionage, cyber conflict, and cyberwar. We provide definitions on these various concepts, based on the definitions of knowledge, data and information that were developed by Lorents (Lorents, 2001, 2008; Lorents, Ottis, & Rikk, 2009).

1. KNOWLEDGE, DATA AND INFORMATION

In order to explain the concept of information we use the definitions of knowledge and data. These definitions are based on the binary relation between such pairs, where the first object is the symbol, sign, name, etc. (notation), of the second object, which, in turn, is the meaning (denotation) of the first object. It is important to note that the notations and denotations are not limited to only things that can be seen or heard by humans (for example, gestures, signs, symbols, texts, pictures, etc.).

Let us agree that if A is the notation for B and, at the same time, B is the denotation of A, then we can represent this relationship as (A ∫ B), or in simple cases as A ∫ B. The symbol "∫ " represents a stylized letter S (referring to words like "signum", "sign", etc.). Let us also agree that if we have formed an ordered pair, where A is the first element and B is the second element, then we represent it as ⟨A,B⟩.

Note that the notation-denotation relationship "∫ " is a fundamental relationship, and therefore it has no definition. This, however, does not mean that we cannot formulate the properties of this relationship. These properties can be represented formally, so they can be considered as logic formulas. There are two types of assertions or arguments (expressed by logic formulas). The first type is considered a priori proven – axioms or postulates that serve as the foundation. The second type consists of all the arguments that can be proven based on previously proven (including a priori proven) arguments.

The properties of the notation-denotation relationship include, but are not limited to:

- *non-uniqueness* (Lorents, 2001). This means that there could be many denotations for a given notation, or many notations for a given denotation. For example, (I∫"Roman number") and (I∫"capital letter i"), or (2∫"two") and (II∫"two").

- *transitivity* (Lorents, 2001). This refers to the property that allows relationships to be "carried over", or in short (A∫B)&(B∫C)→(A∫C).
- *equality (*Lorents, 2005). If two elements are equal (same), then the first element can be used as the notation for the second element, or in short (A=B→(A∫B)). Note that while some things may seem obvious to a human, they still need to be either postulated or proven, in order to consider them correct. For example, it seems that if A=B, then both can be used as notations or denotations for the other. However, this still needs to be proven.

Proof for [X=Y→(X∫Y)&(Y∫X)]:

$$\dfrac{X=Y\to(X\int Y) \qquad\qquad \dfrac{X=Y\to Y=X \qquad Y=X\to(Y\int X)}{X=Y\to(Y\int X)}}{X=Y\to(X\int Y)\,\&\,(Y\int X)}$$

Definition 1. If some objects A and B have the relationship (A∫B), then the ordered pair ⟨A,B⟩ is called knowledge (Lorents, 2001, 2008).

Therefore, if some objects A and B have the relationship (A∫B), we can say that the denotation (meaning) of A is *known*. Similarly, we can say that the notation (symbol, sign etc.) of B is *known*.

Note that knowledge is an ordered pair of some notation and its denotation, not the text (A∫B), which represents the *argument* that A and B have the relationship "∫". At the same time, not every ordered pair is knowledge, even if the elements in it are considered notation and denotation. For example, the ordered pairs ⟨II,2⟩ and ⟨V,5⟩ are knowledge (about the correspondence between Roman and Arabic numbers), but the ordered pair ⟨II,5⟩ is not (in this setting).

Definition 2. D is *data,* if there is an A, so that ⟨A,D⟩ is knowledge or if there is a B, so that ⟨D,B⟩ is knowledge.

From this definition, it follows that only an element (notation or denotation) from some piece of knowledge can be data. For example, data about European countries: there is data that Albania, Andorra, ⋯, and the Vatican are European countries.

Definition 3. Information is either knowledge or data (Lorents et al, 2009).

There are two implications from this definition:

1. something can be information only if it is knowledge or it has a notation or it has a denotation, and

2. if something is not knowledge, notation or denotation, then it is not information.

2. SYSTEMS, INFORMATION SYSTEMS AND INTELLIGENT SYSTEMS

It is possible to operate (for example, input, create, modify, store, systematize, output, transmit, erase, etc.) with information as states or changes of states (in case of time-dependent systems) of systems. By systems we mean a structured set of elements, or more precisely, for a system we need some fixed set of elements (basic set) and a fixed set of properties or relations of these elements (signature) (Cohn, 1965; Grätzer, 2008; Lorents, 2006; Maltsev, 1970). Note that it is *not required* to fix both properties and relations, nor is it required to fix all properties or all relations of the set of elements.

Definition 4. An *information system* is a system (a fixed set of elements and their properties or relations) that is designed to operate with information.

In simpler cases, where the only role of the system (or an object) is to store, present, etc., (to be in the role of a notation or denotation) information, we can say that the system or object *contains information, carries information, possesses information*, etc.

Definition 5. An *intelligent system* is a system that operates with knowledge (Lorents & Lorents, 2003; Lorents, 2008).

An important implication from this definition is that not every information system is an intelligent system. The defining characteristic of an intelligent system is its ability to operate with knowledge. Therefore, the mere presence of knowledge in a system does not automatically mean that the system is intelligent. A printed encyclopedia, for example, only contains information, but does not operate with it, so it is not an intelligent system.

Note that *it does not follow* from the information and intelligent system definitions, that a system which inputs and outputs only data is a “non-intelligent” information system. For example, processing (numeric) input data to get (numeric) output data often requires operations with corresponding knowledge.

Information systems, both man-made technological systems and the humans themselves, can be combined into "systems of information systems", such as cyberspace and cyber society (Lorents et al, 2009; Ottis & Lorents, 2010). Note that the term "cyber" has made a strong comeback after a few decades of relative quiet and regained its standing next to various "info"-related concepts. For example, cyber attacks, cyber defense, cyber weapons, cyber conflicts and cyberwarfare. One way to explain it is that we have witnessed an increased interest in incidents affecting the communication and control of systems that provide the everyday services of modern society. Communication and control, however, characterize the research field of cybernetics, which is the origin of the term "cyber" (Wiener, 1948).

In order to clearly describe and analyze events, it is important that these concepts can also be defined based on a steady foundation of basic terms and principles. This is especially important, if we want to use artificial intelligence to generate correct decisions from a correct description of the situation (which often requires an educated decision that is beyond the capability of the human, in terms of speed, memory, etc.).

3. SECURITY OF INFORMATION

Next we review the three security aspects of information systems – availability, integrity and confidentiality. Depending on the case the emphasis between these aspects may be different. For example, owners of a public news website are mostly concerned with availability and integrity of the displayed information, and not at all interested in maintaining the confidentiality of news stories. On the other hand, the list of double agents in an intelligence agency must be kept confidential, with secondary considerations for integrity and availability.

We also review two special cases of compromising the security of information – destruction and falsification of information.

3.1 AVAILABILITY OF INFORMATION

In the definition for information systems we stated that the system must be able to operate with information. However, in some cases the system may not be able to fulfill this requirement. There are two potential reasons for this:

1. The information that is required to complete the operation is damaged to the point where the system cannot function correctly. For example, a form of malware, called "ransomware", encrypts the files on the victim's system, rendering the system useless (as the victim can no longer access her information) until the owner pays a ransom.

2. The means to complete the operation are damaged or degraded to the point where the system cannot function correctly. For example, a piece of code could have a “memory leak”, writing garbage data on the computer’s memory until the performance of the system begins to degrade.

Remark. In principle, attacks against availability aim to deny the use or the designed functionality of the target system or information.

The “scientific inspiration” for hindering the transfer of information comes from Shannon (1949) and Tuller (1949). Their work gave us the formula for calculating the throughput capacity of an information channel: $W\cdot log_2(1+P/N)$, where W is the available bandwidth, P is the average power of the signal and N is the average power of the noise in the channel.

This, in turn, has led us to the estimation of the maximum information transfer rate: $K£W\cdot log_2(1+P/N)$ (Lorents, 2001b). Therefore, if we increase the power of noise in the channel, we will decrease the information throughput. This principle is applicable for all manner of “jammers”, regardless of technical details. For example, it explains the availability issues resulting from a distributed denial of service attack or a simple e-mail spam flood.

3.2 INTEGRITY OF INFORMATION

In many cases we need to accept the fact that if even one element in a set is added, removed or replaced, then we no longer have the *same* set. This also applies to systems, where in addition to elements we need to worry about the properties or relations of the elements. In case of strictly formalized systems (Grätzer, 2008; Lorents, 2001b, 2006; Maltsev, 1970) the system is considered different even if only one property or relation of an element is added, removed or replaced.

This may not be a problem for a human, but it will affect the decisions of a *correctly* working artificial intelligence system. Therefore, we should discuss damaging or corrupting the integrity of information. Let us agree that:

- the *integrity of information is not compromised* if all (and nothing else) elements, their properties and relations are present *as they are meant to be* (for example, as they are fixed in a design document), and
- in all other cases, the *integrity of information is compromised* (destroyed, corrupted, damaged, etc.)

Remark. In principle, attacks against integrity aim to damage the structure of the target system or information.

Note that one way to corrupt the integrity of information (or destroy it) is to break the notation-denotation relationship (knowledge). Therefore, it is not always necessary to erase or corrupt data.

3.3 CONFIDENTIALITY OF INFORMATION

The confidentiality of information and the concept of secret information rest on the concept of knowledge. In addition, the time when some information must be kept confidential is also important.

Definition 6. Information X, A or B (where $X=\langle A,B\rangle$ and $A \int B$) is *confidential* from system S if system S *cannot be able to acquire* knowledge X during the designated time period (from t_0 to t_1).

Note that in this case it is the fact of (not) acquiring the knowledge that is important. It is also important to pick the time t_1 in such a way that there are no problems if the confidentiality is lost after t_1. For example, the detailed agenda and travel route of a visiting dignitary may need to be confidential (for personal security reasons) until he leaves. After that, the details can be released to the public.

When compared to the destruction of information, we see that instead of removing knowledge (X), notation (A), denotation (B) or the relationship between them ($A \int B$), we need to make it impossible for system S to possess and use (to reconstruct knowledge) them.

3.4 FALSIFYING INFORMATION

Falsifying refers to the process of making some information false. As a result, the integrity and availability of the original information is lost. In order to discuss the concept of falsifying information we need to review some basic terms. First, the concepts of “true” and “false” are in essence assessments. Assigning and using assessments requires answers to three simple questions (Lorents, 2006):

- What objects are assessed?
- What are used as assessments?
- How are assessments assigned to the assessed objects?

Let us agree that we want to assess logic formulas – objects representing arguments and constructed in a highly formal way. Note that the choice and assignment of logical assessments or truth-values is dependent on the underlying logic. For example, in the classical logic, we can use the binary Boolean logic elements (0 and 1), whereas in quantum mechanics we can use three truth-values (Birkhoff & von Neumann, 1936). Non-traditional logic frameworks (with more than two truth-values) are not only theoretical, but can be applied in various practical tasks, such as automatic synthesis of computer programs (Tyugu, 1988, 2007). Note that in case of non-traditional logic frameworks, “not true” may not be “false” and “not false” may not be “true”.

The simplest logic formulas are so-called atomic formulas, which represent either the existence of some property of the elements, or the existence of a relationship between the elements. This group also includes the formula for knowledge – A∫B.

Let us recall that X is information if it is knowledge or data, or in other words:

- there are A and B, so that (A∫B) and X=⟨A,B⟩, or
- there are A and B, so that (A∫B) and X=A, or
- there are A and B, so that (A∫B) and X=B.

Therefore, if we want to claim that X is false, we must find a formula that is false, or at least is not true. In this case, it is the formula A∫B.

Definition 7 (Lorents, 2007). Some information X is *false information,* if:

- there is an argument “there are A and B, so that (A∫B) and X=⟨A,B⟩” while A∫B is *not true*, or
- there is an argument “there are A and B, so that (A∫B) and X=A” while A∫B is *not true*, or
- there is an argument “there are A and B, so that (A∫B) and X=B” while A∫B is *not true*.

Note that there is a difference between false information and non-information. At the same time, it is easy to prove that if X is false, then X is not information.

Proof. $[(\exists\alpha\beta)(P(\alpha,\beta)\&M(\alpha,\beta)\&\neg M(\alpha,\beta)) \vee (\exists\alpha\beta)(R(\alpha)\&M(\alpha,\beta)\&\neg M(\alpha,\beta)) \vee$

$\vee (\exists\alpha\beta)(Q(\beta)\&M(\alpha,\beta)\&\neg M(\alpha,\beta))] \rightarrow$

$\rightarrow \neg[(\exists\alpha\beta)(P(\alpha,\beta)\&M(\alpha,\beta)) \vee (\exists\alpha\beta)(R(\alpha)\&M(\alpha,\beta)) \vee (\exists\alpha\beta)(Q(\beta)\&M(\alpha,\beta))]$

The fact that X is not information does not always mean that X is false. False information can be very useful in information or cyber operations. For example, false information could be used for misleading the enemy about your plans, strengths and weaknesses. On the other hand, it could be used as bait – something that looks correct and credible, but is in fact not useful for the attacker.

3.5 DESTROYING INFORMATION

Destruction of information results in a complete loss of integrity and availability. In order to define information destruction we recall that information is either knowledge or data. Data, in turn, must either have at least one notation or one denotation. Therefore, X can be information only if:

- there are A and B, so that (A∫B) and X=⟨A,B⟩, or
- there are A and B, so that (A∫B) and X=A, or
- there are A and B, so that (A∫B) and X=B.

Theorem. X is not information, if:

- there *are no* A and B, so that (A∫B) and X= ⟨A,B⟩, *and*
- there *are no* A and B, so that (A∫B) and X=A, *and*
- there *are no* A and B, so that (A∫B) and X=B.

Proof. Results directly from Definition 3 and the corresponding Implication 2.

This provides us with the possible ways to destroy information (X):

1. *Destroying the objects A and B*. This will also destroy the ordered pair X= ⟨A,B⟩ and anything that no longer exists is also no longer information. For example, destroying a secret military installation and erasing all references (written or otherwise) to it.

2. *Destroying the notation-denotation relationship between A and B*. This way, the ordered pair X=⟨A,B⟩ may still exist, but it is no longer knowledge, because it lacks the notation-denotation relationship. For example, creating a false identity for Joe Smith. Both the original name (notation) and the original person (denotation) still exist, but the person is no longer associated with the old identity.

3. *Destroying all objects, which are notations or denotations for X*. If X has no notations or denotations, then X is a nameless, pointless thing. For example, if X is knowledge about the password to a particular user account, then erasing that account effectively destroys the value of the password (as knowledge).

4. IT AND CYBER WEAPONS

Let us explore the concept of a weapon in the world of systems. First, it is important to differentiate between *things that may be used as a weapon* and *things that were designed as a weapon*.

Definition 8. A *weapon* is a system that is designed to damage the structure or operations of some other system(s). (Lorents, 1998)

Weapons can include systems that deal kinetic, thermal and electromagnetic damage, as well as chemical compounds and biological organisms, etc. Therefore, it should not be surprising that there can also be weapons that work in the information systems.

Definition 9. An *information technology weapon*, or shorter – *IT weapon*, is an information technology-based system (consisting of hardware, software and communication medium) that is designed to damage the structure or operations of some other system(s).

For example, an IT system that is designed to analyze the sensor feeds to provide an accurate location for an enemy tank (to be destroyed by missiles) can be called an IT weapon.

Definition 10. A *cyber weapon* is an information technology-based system that is designed to damage the structure or operations of some other information technology-based system(s).

For example, a software tool that allows generating unnecessary network traffic for a web server is a cyber weapon. Similarly, a software tool that is designed to copy confidential user information (for example, login credentials) without the knowledge and consent of the user is a cyber weapon, because it breaches the (presumed) confidentiality requirement of the system's operations.

Note that every cyber weapon is also an IT weapon, but the opposite is not true. The targets of cyber weapons are located in cyberspace, which reinforces the connection with the "cyber" prefix.

5. CYBER INCIDENTS, ATTACKS, CONFLICTS AND WAR

The core concept in information technology is naturally information. It is both the key protected asset and the key target in the contested ground of cyberspace. Therefore, we provide the important definitions for offensive cyber operations.

Definition 11. Cyber incidents are events that cause or may cause unacceptable deviation(s) in the structure or operation of an information system (or its components, including information, hardware, software, etc.).

Cyber incidents can be accidental (for example, a power outage causes the system to stop working) or intentional. Furthermore, they can be the effects from events in cyberspace or physical effects.

Definition 12. Cyber attack is the intentional use of a cyber weapon or a system that can be used as a cyber weapon against an information system in order to create a cyber incident.

For example, launching a distributed denial of service attack with a botnet, or infecting target systems with malware that disables them.

Definition 13. Cyber espionage is the use of cyber attacks to cause a loss of confidentiality of the target system.

For example, exploiting a vulnerability in the target system's configuration to gain access to confidential files.

Definition 14. Cyber conflict is the use of cyber attacks (which must include attacks against integrity or availability of the target systems) to achieve political aims.

The requirement for integrity or availability attacks comes from the fact that cyber conflicts are different from cyber espionage. While espionage can also be part of a cyber conflict, it can exist separately (and often does). Conflict, however, implies activities that either damage the target (integrity) or make it unusable (availability). The political aim in this definition is an umbrella term that is meant to include nationalism, religion, philosophy, etc., as the underlying reason for the conflict. An example of cyber conflict is the cyber attack campaign against Estonia in 2007.

Definition 15. Cyberwar is a cyber conflict between state actors.

While cyber conflicts can take place between state actors, non-state groups and individuals, a war is limited to state actors. For example, military specialists using cyber attacks to disable enemy command and control systems before a decisive ground and air attack.

Note that in this definition we are not necessarily concerned with the definition of warfare provided by contemporary international law, which may or may not be applicable to conflicts in cyberspace, depending on the interpretation (Schmitt, 1999, 2002). Instead, we provide the definition as part of a conceptual framework.

6. SUMMARY

Cyber attacks can be used in new forms of expression and conflict. In order to describe and study these events, we need a solid framework of definitions. In this paper we have covered the basic concepts of knowledge, data and information. From this, we provided definitions for information systems and intelligent systems, as well as information technology weapons and cyber weapons. With this foundation in place, we explored the three basic concepts of securing information systems – confidentiality, integrity and availability, and included two special cases of breaking these concepts: destruction and falsification of information. Lastly, we provided definitions for the concepts of cyber incident, cyber attack, cyber espionage, cyber conflict and cyberwar.

REFERENCES

- Birkhoff, G., von Neumann, J., 1936. The logic of quantum mechanics. *Ann. Math*. 37, 823–842.
- Cohn P. M., 1965. *Universal Algebra*. Evanston: Harper&Row.
- Grätzer, G., 2008. *Universal Algebra*. Second Edition. Springer.
- Hartley, R. V. L., 1928. Transmission of Information. *BSTJ* 7, 3, pp 535-563.
- Lorents, P., 1998. *Süsteemse käsitluse alused. Riigikaitse ja julgeoleku põhiküsimused.* (Foundations of the Systemic Approach. Main Problems of National Defence and Security.) Tallinn: Eesti Riigikaitse Akadeemia kirjastus.
- Lorents, P., 2001. Formalization of data and knowledge based on the fundamental notation-denotation relation. *Proceedings of the International Conference on Artificial Intelligence*. IC – AI' 2001. Vol III, pp 1297-1301.
- Lorents, P., 2001b. *Informaatika teoreetilised alused. Struktuurne aspekt*. (Theoretical Foundation of Informatics. Structural Aspect.). Tallinn: EBS Print.
- Lorents, P., & Lorents, D., 2003. Intelligence and the notation-denotation relation. *Proceedings of the International Conference on Artificial Intelligence*. IC – AI' 2003. Vol II, pp 703-707.
- Lorents, P., 2005. The role of equality in knowledge acquisition. *Proceedings of the International Conference on Artificial Intelligence*. IC – AI' 2005. Vol II, pp 555-561.
- Lorents, P., 2006. *Süsteemide maailm* (The World of Systems). Tartu: Tartu Ülikooli Kirjastus.
- Lorents, P., 2007. Denotations, Knowledge and Lies. *Proceedings of the International Conference on Artificial Intelligence*. IC-AI' 2007. Las Vegas, US, June 14-17, Vol II, pp 324-329. CSREA Press.
- Lorents, P., 2008. Knowledge and Taxonomy of Intellect. *Proceedings of the International Conference on Artificial Intelligence*. IC-AI' 2007. Las Vegas, US, July 25-28, Vol II, pp 484-489. CSREA Press.
- Lorents, P., Ottis, R., Rikk, R., 2009. Cyber Society and Cooperative Cyber Defence. *Internationalization, Design and Global Development*. Lecture Notes in Computer Science, Vol 5623, pp 180-186.
- Maltsev, A. I. (Мальцев А. И.), 1970. *Алгебраические системы* (Algebraic systems). Moscow: Наука.
- Ottis, R., & Lorents, P., 2010. Cyberspace: Definition and Implications. *Proceedings of the 5th International Conference on Information Warfare and Security*. ICIW 2010. Dayton, US, 8-9 April. [accepted for publication]
- Schmitt, M., 1999. Computer Network Attack and Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, Vol 37, pp 885-937.
- Schmitt, M., 2002. Wired warfare: Computer network attack and jus in bello. *International Review of the Red Cross*, Vol 84, No 846, pp 365-399.
- Shannon, C. E., 1949. Communication in the presence of noise. *PIRE*, 37, 1, pp 10-21.
- Tuller, W. G., 1949. Theoretical limitations on the rate of transmissioon of information. *PIRE*, 37, 5, pp 468-478.
- Tyugu, E., 1988. *Knowledge-Based Programming*. London: Addison-Wesley.
- Tyugu, E., 2007. *Algorithms and Architectures of Artificial Intelligence*. Amsterdam: IOS Press.
- Wiener, N., 1948 *Cybernetics: Or Control and Communication in the Animal and the Machine*. New York: John Wiley.