Cyberspace and cyber warfare Cyberspace and cyber warfare

Martti Lehto
University of Jyväskylä

Cyberspace and cyber warfare

2018

Martti Lehto, University of Jyväskylä, Jyväskylä, Finland

Originally published in K. Dimitrov (Edit.) Cyber Defence in Industry 4.0 Systems and Related Logistics and IT Infrastructures, NATO Science for Peace and Security Series D: Information and Communication Security, Vol 51, pages 99-109, 2018

Cyberspace and cyber warfare

Martti Lehto
Faculty of Information Technology, University of Jyväskylä, Finland
martti.j.lehto@jyu.fi

Abstract
This chapter describes and evaluates the cyber world, including its phenomena, from a strategic perspective. As no universally accepted definitions for the cyber world exist, associated literature and publications address it in many ways. This chapter depicts the standards-based risk model, cyber operations and cyberweaponry, as well as the critical structures of society as the targets. Moreover, cyber security definitions and a five-layer model of cyber threats, which include cyber vandalism, cybercrime, cyber intelligence, cyberterrorism and cyberwarfare are provided.

Keywords: Cyber space, cyber warfare, cyber operations, cyber threats, cyber security

1. Introduction

The word *cyber* is generally believed to originate from the Greek verb κυβερεω (kybereo) - to steer, to guide, to control. At the end of the 1940s Norbert Wiener (1894–1964), an American mathematician, began to use the word *cybernetics* to describe computerised control systems. According to Wiener, cybernetics deals with sciences that address the control of machines and living organisms through communication and feedback. Pursuant to the cybernetic paradigm, information sharing, and manipulation are used in controlling biological, physical and chemical systems. [25] [29]

Many countries are defining what they mean by cyber world or cyber security in their national strategy documents. The common theme from all of these varying definitions, however, is that cyber security is fundamental to both protecting government secrets and enabling national defense, in addition to protecting the critical infrastructures that permeate and drive the 21st century global economy.

There are terms and concepts associated with cyberspace which are difficult to define due to the very nature of cyberspace and different phenomena therein. Cyberspace is a man-made ecosystem. While land, air, sea and space domains exist without any human presence, cyberspace requires continuous human attendance and activities. Cyberspace fuses all ICT networks, databases and sources of information into a global virtual system. Cyberspace structures include the economy, politics, armed forces, psychology and information [12]. Some researchers also include societal and infrastructure domains in cyberspace. Nonetheless, the Internet is an integral and elemental part of this new world.

Cyberspace is more than the internet, including not only hardware, software, data and information systems, but also people and social interaction within these networks and the whole infrastructure. The International Telecommunication Union (ITU) uses the term to describe the "systems and services connected either directly to or indirectly to the internet, telecommunications and computer networks.” [15] The International Organisation for Standardisation (ISO) defining cyber as “the complex environment resulting from the interaction of people, software and services on the internet by means of technology devices and networks connected to it, which does not exist in any physical form.” [14]

The US Joint Publication 3-12R says that “Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.” [7]

To sum up, the cyber world can be defined as a global and multidimensional ICT network, into which the user (man or machine) can connect via fixed or mobile data terminals, and virtually move about within it. In other words, the cyber world is an amalgamation of the Internet, other physical networks, digital services and virtual reality: it is a multi-user virtual environment.

1. Cyber threats and vulnerabilities

1.1. Cyber threats

Threats to society’s vital functions may directly or indirectly target national systems and/or citizens, from within or outside the national borders. The threat landscape is a list of threats containing information about threat agents and attack vectors. By exploiting weaknesses/vulnerabilities, threats may lead to a loss or takeover of assets. The threats to society’s vital functions can be divided into three entities which are: physical threats, economic threats and cyber threats.

Threats in cyberspace can be classified in many ways. The threat landscape is a list of threats containing information about threat agents and attack vectors. By exploiting weaknesses/vulnerabilities, threats may lead to a loss or takeover of assets.

The European Network and Information Security Agency (ENISA) uses a cyber threat model consisting of threats. The threats include different forms of attacks and techniques as well as malware and physical threats. In the ENISA-model “a threat agent is any person or thing that acts (or has the power to act) to cause, carry, transmit, or support a threat”. Some of the major threat agents in cyberspace are corporations, cybercriminals, employees, hacktivists, nation states, and terrorists. [10]

One of the common threat models is a fivefold classification based on motivational factors: cyber vandalism, cybercrime, cyber espionage, cyber terrorism and cyber warfare. With a typology such as these motives can reduce to their very essence: egoism, anarchy, money, destruction and power. [8] [1]

Level 1 consists of cyber vandalism which encompasses hacking and hacktivism. For a single company or an individual their activities can cause significant economic losses.

Level 2 consists of cybercrime. The Commission of the European Communities defines cybercrime as “criminal acts committed using electronic communications networks and information systems or against such networks and systems" [5]

Level 3 consists of cyber espionage. This can be defined as action aimed at obtaining secret information (sensitive, proprietary or classified) from individuals, competitors, groups, governments and adversaries for the purpose of accruing political, military or economic gain by employing illicit techniques in the Internet, networks, programs or computers. [18]

Level 4 consists of cyber terrorism which utilizes networks in attacks against critical ICT systems and their controls. The purpose of the attacks is to cause damage and raise fear among the general public, and to force the political leadership to give into the terrorists’ demands. [2]

Level 5 is cyber warfare, which has universally accepted definition for cyber warfare exists; it is quite liberally being used to describe the operations of state-actors in cyberspace. Cyber warfare *per se* requires a state of war between states, with cyber operations being but a part of other military operations.

1.2. Cyber world vulnerabilities

Threat, vulnerability and risk form an intertwined entirety in the cyber world. First, there is a valuable physical object, competence or some other immaterial right which needs protection and safeguarding. A threat is a harmful cyber event which may occur. The numeric value of the threat represents its degree of probability. Vulnerability is the inherent weakness in the system which increases the probability of an occurrence or exacerbates its consequences. Vulnerabilities can be divided into those that exist in human action, processes or technologies. Risk is the value of the expected damage. Risk equals probability times the loss. It can be assessed from the viewpoint of its economic consequences or loss of face. Risk management consists of the following factors: risk assumption, risk alleviation, risk avoidance, risk limitation, risk planning and risk transference. Countermeasures can be grouped into the three following categories: regulation, organizational solutions (management, security processes, methods and procedures and the security culture) and security technology solutions.

2. Cyber warfare

2.1. Cyber Warfare definition

As there is no generally accepted definition for cyber warfare it is quite liberally used in describing events and action in the digital cyber world. The concept of cyber warfare became extremely popular from 2008-2010, partly superseding the previously used concept of information warfare which was launched in the 1990s. For some, cyber warfare is war which is conducted in the virtual domain. For others, it is a counterpart of conventional ‘kinetic’ warfare. According to the OECD’s report, cyberwar military doctrines resemble those of so-called conventional war: retaliation and deterrence. Researchers agree with the notion that the definition of cyberwar should address the aims and motives of war, rather than the forms of cyber operations. They believe that war is always widespread and encompasses all forms of warfare. Hence, cyber warfare is but one form of waging war, used alongside kinetic attacks. [23]

The new capacities of armed forces create new possibilities, both the kinetic and non-kinetic use of force in cyberspace. Cyber era capabilities make possible operations in the new non-linear and indefinite hybrid cyber battlespace. It must be possible to seamlessly integrate the decision-makers, actors and all types of manned and unmanned platforms in the air, on the surface, under the surface, in space and in cyberspace. The main trends that are changing the cyber battlespace are networking, time shortening, the increasing amount of data, proliferation of autonomous and robotic systems as well as artificial intelligence and cognitive computing. [19] [20]

Cyber warfare, in its present form, can be understood to incorporate both IW and EW, thereby establishing a modus operandi that complies with network centric warfare. Cyber-thinking hopes to bring the structures of cyberspace, i.e. the critical infrastructure, alongside information that is at the core of the information environment. All vital functions of society are more or less networked. Being ‘networked’ refers to action which is not fixed to any time or place and the management of functions. Network structures, along with information, are gaining in prominence. Yet another significant paradigm shift is the fact that while information warfare is generally perceived to occur during conflicts and war, nowadays cyber threats – in all their different forms – have become a part of everyday life for people and institutions. [19] [20]

Cyber warfare can be divided into strategic and operational-tactical warfare, depending on the role assigned to cyber operations in the different phases of war. State actors launch offensive cyber operations in situations where the states are not at war with each other. In this case, the cyber-attacks constitute a cyber conflict in a low intensity conflict, as was the case with Estonia in 2007.

In the spring of 2007 Estonia was subjected to a three-week long series of cyber-attacks which targeted, among others, the government, the police, the banking system, the media and the business community. The cyber campaign mainly used denial of service (DOS) attacks targeting among other things web servers, e-mail servers, DNS servers and routers. [24]

The Russo-Georgian War, also known as the South Ossetia War, was fought during the first week of August 2008 between Georgia and the Russian Federation, and the army of the Republic of South Ossetia. In this short-lived war cyberwarfare was used as a part of conventional ‘kinetic’ operations. As early as 8 August several Georgian and South Ossetian websites experienced DOS attacks. The campaign against Georgian websites began on the night of August the 9th. The attacks targeted the websites of Georgia’s government and President, and *Georgia-online*. On 11 August the Georgian authorities decided to fight the ‘disinformation’ and stopped all Russian TV broadcasts in the country. Caucasus Online, Georgia’s leading Internet service provider, prevented access to all pages that had a *.ru* Internet domain suffix. The Russian *RIA Novosti* news agency’s website was attacked and went down for a few hours on 10 August. The website of Russia’s English-speaking TV channel *RussiaToday* was attacked on 12 August and remained inoperative for approximately 24 hours. Hackers gained access to the web pages of Georgia’s

Central Bank and the Ministry of Defence and tampered with some media footage in them.

Martin Libicki argues that a cyber-attack used in lieu of kinetic methods creates more ambiguity in terms of effects, sources, and motives. The cyber-attacks change the risk profile of certain actions, and usually in ways that make them more attractive options. He presents four hypothetical uses of cyber-attacks. One, cyber-attacks may be used by a victim of small-scale aggression to indicate its displeasure but with less risk of escalation than a physical response would entail. A state rich in cyber warriors may also use the threat of cyber war to deter the potential target against support proxy war fighters. Cyber-attacks can be used by one state to affect the outcome of conflict in another state without having to make any sort of visible commitment, even an implied one. Cyber-attacks do not need to be directed towards adversaries, although the risks of making new enemies if the source of the cyber-attacks is discovered are obvious. [21]

2.2. Cyberspace Operations

Within the United States military domain Cyberspace operations (CO) are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Cyberspace superiority is the degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary. [7]

The execution of CO requires the integrated and synchronized employment of offensive, defensive, operations, underpinned by effective and timely operational preparation of the environment. CO missions are categorized as offensive cyberspace operations (OCO) and defensive cyberspace operations (DCO) and Armed Forces information network operations (in US eg. DODIN) [7]. We can add also cyber intelligence operations as a part of CO.

Defensive cyberspace operations are defined as passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. Offensive cyberspace operations intended to project power by the application of force in or through cyberspace. Information network operations are operations to design, build, configure, secure, operate, maintain, and sustain Armed Force's networks to create and preserve information assurance on the information networks. [7] Cyber intelligence operations include enabling actions and intelligence collection via computer networks that exploit data gathered from target or enemy information systems or networks.

The present warfare is totally dependent on the C5ISR system (command-control-communicatio-computers-cyber-intelligence-surveillance-reconnaisance). The command and control, coordination and communication of the military operations require functional C5ISR system. The C5ISR system is the most vulnerable part and therefore it should be the most important object of the cyber defence of armed forces. The C5ISR system of today's defence systems is complex wholeness from the radios, radars, mainframes, to the PC devices and to the embedded and cyber-physical systems. The C5ISR system uses the data networks of armed forces, and in addition the internet, civilian networks, wireless solutions, navigation systems and radio networks of the wide frequency range. Networked C5ISR system contains also a huge variety of vulnerabilities. The hostile penetration is possible in any given part of the system and the attack can cause problems to the radar surveillance, telecommunications or air defence system. It can paralyze the fire control system, positioning system, satellite or the mobile communication systems. The complexity of the system makes impossible to totally eliminate the vulnerabilities and to identify and to track the penetrations inside the system. The networking increases efficiency of the defence systems but at the same time more dangerous vulnerabilities arise.

2.3. Cyber weaponry

A cyber weapon refers to a computer program which operates in computers other than those of the user, in the same vein as a computer virus. While a cyber-weapon, by its design, can be an independently mobile and spreading virus, mobility is not a necessary precondition. The most successful cyber weapons are phlegmatic by nature, being either nearly or totally inert in the local area network. In the latter case the cyber weapon must specifically be infiltrated into each target. [16]

The detected cyber weaponry such as Stuxnet and its kin, *Flame*, *Duqu* and *Gauss*, are all modular malware. The desired functionality of such malware is constructed from several process objects. Of these, the clearly identifiable ones include its ‘warhead’, the malware payload, and its platform, the delivery module. [16]

The platform is controlled by a *command, control and communication module* (C3) which operates independently or in contact with its command and control servers, receiving further commands from them. This module targets and activates the warhead components and it may also download new warheads from its command and control servers. The module also controls the mobility of the cyber weapon. Stuxnet was discovered because of a flaw in the command, control and communication module which made it spread more rapidly than originally intended. [16]

In order to break through to its target the weapon carries one or more *exploit modules* which are programmed to exploit system vulnerabilities. There are many kinds of vulnerabilities. For example, one may permit the installation of program code into network software in such a manner that it begins to execute the code. A different vulnerability may arise from a standard password in an automated system. By exploiting these vulnerabilities, the cyber weapon seizes partial control over the targeted system and, having gained a toehold, manages to re-distribute itself across the system. [16]

With the help of the attack modules the *mobility and installation modules* implement the actual replication and mobility of the malware, installing the weapon into the target computer’s operating system. The known cyber weapons can exploit the operating system manufacturers’ certificates; this makes it possible for them to quite stealthily be installed as bona fide device drivers or library code. A cyber weapon may also contain an installable rootkit functionality which activates at this stage. It affects the operating system by obscuring the cyber weapon's ongoing processes and files in the computer's file system during system check. [16]

If the cyber weapon is designed to spread in the target organisation's LAN, one must first manage to insert it into the firewall-protected network. This can be achieved, for example, via infected USB flash drives or by e-mailing the cyber weapon to its target, as was the case with the Duqu Trojan. In such an instance the weapon burrows into its target by means of a *dropper* package which may outwardly appear to be a word processing document, for example. [16]

Then the delivery vehicle, constructed of the abovementioned modules, will inject one or more actual warheads into the target. One warhead may carry out intelligence, seeking certain kinds of files from the target computer or network servers, hijacking typed passwords from keyboards or eavesdropping on the room through the computer's microphone, etc. Another warhead may cause harm, searching and destroying automated systems, disrupting databases and causing other such damage. [16]

Figure 1 illustrates the design of a standard cyber weapon.

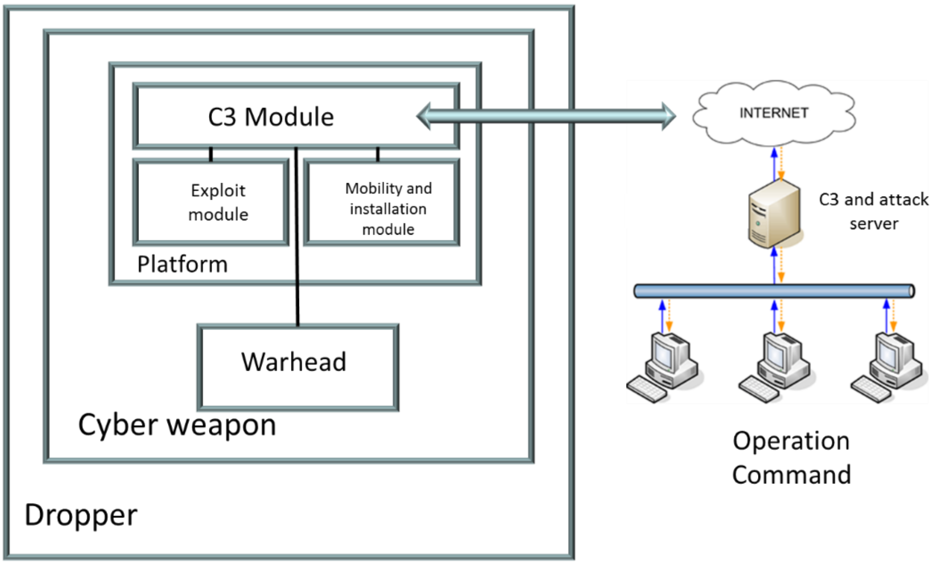

Figure 1. A standard cyber weapon

2.4. Society's critical structures as targets

In the cyber world the most important threat focuses on critical infrastructure (CI). CI encompasses the structures and functions which are vital to society's uninterrupted functioning. It comprises physical facilities and structures as well as electronic functions and services. In order to secure them, one must identify and protect individual critical targets while constantly keeping an eye on the functioning of the infrastructure as a whole. [13]

Most countries have a detailed definition regarding their critical infrastructure, including its importance to society, associated threats, its different parts and sectors, and often also the manner by which it is safeguarded. The definitions have normally seen the light of day in conjunction with new, internal security-related legislation.

In most countries, this definition has evolved over the years to include an ever-broader range of infrastructures. National definitions differ slightly in the criteria used to define the criticality of an infrastructure. Most countries and institutions use crosscutting criteria, which cover all infrastructures in all sectors. In Germany critical infrastructure are those "facilities and organizations of major importance to the community whose failure or impairment would cause a sustained shortage of supplies, significant disruptions to public order or other dramatic consequences" [17].

In United States nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital to public confidence and the Nation's safety, prosperity, and well-being. [26]

The Nation's critical infrastructure is diverse and complex. It includes distributed networks, varied organizational structures and operating models (including multinational ownership), interdependent functions and systems in both the physical space and cyberspace, and governance constructs that involve multi-level authorities, responsibilities, and regulations. This directive identifies 16 critical infrastructure sectors. [26] The sectors are as follows:

1. Chemical
2. Commercial Facilities
3. Communications
4. Critical Manufacturing
5. Dams
6. Defense Industrial Base
7. Emergency Services
8. Energy
9. Financial Services
10. Food and Agriculture
11. Government Facilities
12. Healthcare and Public Health
13. Information Technology
14. Nuclear Reactors, Materials, and Waste
15. Transportation Systems
16. Water and Wastewater Systems

It is possible to identify three dimensions in safeguarding CI: political, economic and technical. The political dimension arises from different countries' shared interests in securing their CI systems and the ensuing increased mutual cooperation. The political dimension entails national legislation and national security needs as well as associated international cooperation around these two topics. International cooperation aims to achieve analogous solutions in countries whose needs are comparable. Uniform security legislation and security policies facilitate technical cooperation, especially when several countries have shared infrastructure. The economic dimension affects all companies and business actors which build, own and administer infrastructure systems and installations, and whose operations are driven by economic interests. The economic dimension also includes a fair apportionment of security costs between the stakeholders. The technical dimension encompasses technological advances, including their utilisation, and all practical solutions and measures which states, and businesses incorporate in securing the functioning of their critical infrastructure during possible disruptions. [13]

The abovementioned networks are not isolated entities. Rather, they form the national critical infrastructure network within which many interdependencies exist. Should one system be paralysed or collapse, there would be knock-on effects elsewhere in the network. Therefore, the analysis of CI requires modelling so as to determine the interdependencies between the different elements in the network. [27]

According to EU Council Directive 2008/114/EC ‘critical infrastructure’ means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions. [6] [11]

3. Cyber security

Cyber security measures are associated with managing risks, patching vulnerabilities and improving system resilience. Key research subjects include techniques associated with detecting different network behavior anomalies and malware, and IT questions related to IT security. Since these research subjects mainly concentrate on the physical, syntactic and semantic layers, present research infrastructures are focused on studying phenomena in the aforementioned layers.

In short, cyber security can be defined as a range of actions taken in defence against cyber-attacks and their consequences and includes implementing the required countermeasures. Cyber security is built on the threat analysis of an organisation or institution. The structure and elements of an organisation’s cyber security strategy and its implementation programme are based on the estimated threats and risk analyses. In many cases it becomes necessary to prepare several targeted cyber security strategies and guidelines for an organisation.

According to ITU the Cyber security is not an end unto itself; cyber security as a means to an end. The goal should be to build confidence and trust that critical information infrastructure would work reliably and continue to support national interests even when under attack. Therefore, the focus of national cyber security strategies should be on the threats most likely to disrupt vital functions of society. [15]

Conclusion

Cyber power is critically important in joint warfare. Military cyberspace operations should have as their priority the attainment and maintenance of cyber superiority and cyber interdiction in support of kinetic operations. Additionally, operations to gain and maintain cyber superiority should concentrate on neutralizing enemy cyber-attack and cyber reconnaissance capabilities, followed by suppressing enemy cyber defenses. Together, cyberspace superiority and cyber interdiction yield a powerful decision-making advantage in joint warfare, the cumulative effect of which is to compel an enemy to make mistakes that will likely prove fatal in due course. [3]

We must understand the threat of cyber war. State actors, non-state actors or individuals can attack a nation in cyberspace due to the low cost of entry as well as the attribution challenges. State actors will continue to pursue asymmetric advantages using cyberspace in future conflicts through intelligence gathering and deception operations as well as physical cyberspace attacks. [4]

Military operations entail careful target analysis on the adversary's centers of gravity, nodes and vital vulnerable targets. Only by employing such a comprehensive approach can battle commanders at every level fathom how they can best achieve their strategic goals through kinetic and non-kinetic operations. The operations will be successful if the adversary's vital nodes are attacked with all possible kinetic and non-kinetic instruments. By doing so, it is possible to eliminate the adversary's ability to adapt to the situation and make him believe that he will sustain strikes all the way from the physical layer to the cognitive. [28]

References

[1] Ashenden Debi, *Cyber Security: Time for Engagement and Debate*, Proceedings of the 10th European Conference on Information Warfare and Security, the Institute of Cybernetics at the Tallinn University of Technology Tallinn, Estonia, 2011

[2] Beggs Christopher*, Proposed Risk Minimization Measures for Cyber-Terrorism and SCADA Networks in Australia*, Proceedings of the 5th European Conference on Information Warfare and Security, National Defence College, Helsinki, Finland, 2006

[3] Bonner III, Ernest L., *Cyberpower Learning from the Rich Historical Experience of War*, International Conference on Information Warfare and Security, p. 351-IX, 2012

[4] Cahanin Steven E. (2012) Principles of War for Cyberspace, Air War College Maxwell Paper No. 61 Maxwell Air Force Base

[5] Commission of the European Communities, *Towards a general policy on the fight against cyber crime*, Brussels, 22.5.2007, COM(2007) 267 final, 2007

[6] Council Directive 2008/114/EC, *On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, 8 December 2008

[7] Cyberspace Operations JP 3-12(R), 5 February 2013

[8] Dunn Cavelty, Myriam, *The Reality and Future of Cyberwar*, Parliamentary Brief, 30th March 2010

[9] Dunn Cavelty Myriam*, Unraveling the Stuxnet Effect: Of Much Persistence and Little Change in the Cyber Threats Debate*, Military and Strategic Affairs, Vol. No. 3, 2011

[10] ENISA, *Threat Landscape, Responding to the Evolving Threat Environment*, September 2012

[11] EU, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013 JOIN(2013) 1 final JOINT, 2013

[12] Grobler Marthie, van Vuuren Joey Jansen and Zaaiman Jannie, Evaluating Cyber Security Awareness in South Africa, Proceedings of the 10th European Conference on Information Warfare and Security, the Institute of Cybernetics at the Tallinn University of Technology Tallinn, Estonia, 2011

[13] HVK, (National Emergency Supply Agency, http://www.huoltovarmuus.fi/tietoa-huoltovarmuudesta/kriittinen-infrastruktuuri-kasite/, 2013

[14] ISO/IEC 15408:2005, *Information technology - Security techniques - Evaluation criteria for IT security*, 2005

[15] ITU, *ITU National Cybersecurity Strategy Guide*, Geneva 2011

[16] Kiravuo Timo, Särelä Mikko ja Manner Jukka, *Kybersodan taistelukentät*, Sotilasaikakauslehti 3/2013

[17] KRITIS, *National Strategy for Critical Infrastructure Protection (CIP Strategy)*, Federal Republic of Germany, Berlin, 17th June 2009

[18] Liaropoulos Andrew, *War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory*, Proceedings of the 9th European Conference on Information Warfare and Security, Department of Applied Informatics University of Macedonia Thessaloniki Greece, 2010

[19] Libicki Martin C., *What Is Information Warfare?,* Strategic Forum, Number 28 May 1995

[20] Libicki Martin C., *Conquest in Cyberspace – National Security and Information Warfare*, Cambridge University Press, New York, 2007

[21] Libicki Martin C., The Strategic Uses of Ambiguity in Cyberspace in the Military and Strategic Affairs, Vol. No. 3, 2011

[22] McCaughey Martha, Ayers Michael D.*, Cyberactivism: Online Activism in Theory and Practice*, Routledge, New York, 2003

[23] OECD, *IFP Project on Future Global Shocks*, in report: Reducing Systemic Cybersecurity Risk, 14.1.2001

[24] Ottis Rain, *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*, Proceedings of the 7th European Conference on Information Warfare and Security University of Plymouth, UK, 2008

[25] Porter Arthur, *Cybernetics simplified*, English University Press, London 1969

[26] Presidential Policy Directive - *Critical Infrastructure Security and Resilience/PPD-21*, Order 13636 of February 12, 2013

[27] Pye Graeme and Warren Matthew, *Analysis and Modelling of Critical Infrastructure Systems*, Proceedings of the 10th European Conference on Information Warfare and Security, The Institute of Cybernetics at the Tallinn University of Technology Tallinn, Estonia, 2011

[28] Shanahan John N.T., *Shock-Based Operations, New Wine in an Old Jar*, Air & Space Power Journal, 2001

[29] Ståhle Pirjo, Itseuudistumisen dynamiikka - systeemiajattelu kehitysprosessien ymmärtämisen perustana, http://www.stahle.fi/itseuudistumisen_dynamiikka.pdf, 2004