The Cyberspace Threats and Cyber Security Objectives in the Cyber Security Strategies

Martti Lehto, University of Jyväskylä, Jyväskylä, Finland

ABSTRACT

Threats in cyberspace can be classified in many ways. This is evident when you look at cyber security on a multinational level. One of the most common models is a threefold classification based on motivational factors. Most nations use this model as a foundation when creating a strategy to handle cyber security threats as it pertains to them. This paper will use the five level model: cyber activism, cybercrime, cyber espionage, cyber terrorism and cyber warfare. The National Cyber Security Strategy defines articulates the overall aim and objectives of the nation's cyber security policy and sets out the strategic priorities that the national government will pursue to achieve these objectives. The Cyber Security Strategy also describes the key objectives that will be undertaken through a comprehensive body of work across the nation to achieve these strategic priorities. Cyberspace underpins almost every facet of the national functions vital to society and provides critical support for areas like critical infrastructure, economy, public safety, and national security. National governments aim at making a substantial contribution to secure cyberspace and they have different focus areas in the cyber ecosystem. In this context the level of cyber security reached is the sum of all national and international measures taken to protect all activities in the cyber ecosystem. This paper will analyze the cyber security threats, vulnerabilities and cyber weaponry and the cyber security objectives of the Cyber Security Strategies made by Australia, Canada, Czech Republic, Estonia, Finland, Germany, the Netherlands, the United Kingdom and the United States.

Keywords: Cyber Definition, Cyber Security Strategy, Cyber Threats, Cyber Vulnerability, Cyber Weaponry

1. WHAT DOES 'CYBER' MEAN?

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. Cybernetics only applies to machine-like systems in which the function-

DOI: 10.4018/ijcwt.2013070101

ing of the system and the end result can be mathematically modelled and determined, or at least predicted. The cybernetic system is a closed system, exchanging neither energy nor matter with its environment. (Porter, 1969, Ståhle, 2004)

The prefix cyber is often seen in conjunction with computers and robots. William Gibson, a science-fiction novelist, coined the term *cyberspace* in his novel Neuromancer (Gibson 1984). Science-fiction literature and movies portray the Gibsonian cyberspace, or matrix, as a global, computerised information network in which the data are coded in a three-dimensional, multi-coloured form. Users enter cyberspace via a computer interface, where after they can 'fly' through cyberspace as avatars or explore urban areas by entering the buildings depicted by the data.

Cyber, as a concept, can be perceived through the following conceptual model (Kuusisto, 2012):

- **Cyber world:** The presence of human post-modern existence on earth;
- **Cyberspace:** A dynamic artefactual state formed by bits (vs. static);
- **Cyber domain:** A precisely delineated domain controlled by somebody; and
- **Cyber culture:** The entirety of the mental and physical cyberspace-related achievements of a community or of all of humankind.

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.

The Australian cyber security strategy defines cyberspace on the foundation of Australia's digital economy and the importance and benefits of ICT to the entire national economy. In accordance with the strategy "Australia's national security, economic prosperity and social wellbeing are critically dependent upon the availability, integrity and confidentiality of a range of information and communications technologies (ICT). This includes desktop computers, the Internet, mobile communications devices and other computer systems and networks." In short, it is all about the world of networks and terminals.

The Canadian cyber security strategy starts out with the definition of cyberspace: "Cyberspace is the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 1.7 billion people are linked together to exchange ideas, services and friendship." Cyberspace is not only limited to physical networks; rather, it is a world consisting of the exchange of information, communication and different services.

The cyber security strategy of the Czech Republic does not explicitly define cyberspace. It states that "The strategy focuses mainly on unimpeded access to services, data integrity and confidentiality of the Czech Republic's cyberspace and is coordinated with other related strategies and concepts." This definition complies with the traditional data security definition which focuses on the availability, integrity and confidentiality of information.

Strictly speaking, Estonia's cyber security strategy does not define cyberspace. A definition of a kind can be found in the descriptions of the implementation of cyber security. "The security of cyberspace acquires a global dimension and the protection of critical information systems must be elevated, in terms of national security, on a par with traditional defence interests." Furthermore, the strategy states that "the security of the Internet is vital to ensuring cyber security, since most of cyberspace is Internet-based." The strategy introduces networks, users and the information content into cyberspace. "It is an essential precondition for the securing of cyberspace that every operator of a computer, computer network or information system realises the personal responsibility of using the data and instruments of communication."

Finland's cyber security strategy succinctly states: "Cyber domain means an electronic information (data) processing domain comprising of one or several information technology infrastructures. It is stated as an addition, that "representative to the environment is the utilisation of electronics and the electromagnetic spectrum for the purpose of storing, processing and transferring data and information via telecommunications networks."

In Germany's cyber security strategy "Cyberspace is the virtual space of all IT systems linked at data level on a global scale. The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks. Cyberspace includes all information infrastructures accessible via the Internet beyond all territorial boundaries."

The Netherlands' cyber security strategy does not specifically define cyberspace. The section that details cyber security also includes a definition of some kind over cyberspace. "Cyber security is freedom from danger or damage due to the disruption, breakdown, or misuse of ICT. The danger or damage resulting from disruption, breakdown, or misuse may consist of limitations to the availability or reliability of ICT, breaches of the confidentiality of information stored on ICT media, or damage to the integrity of that information." This description follows the traditional data security perspective.

The United Kingdom clearly defines cyberspace: "Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the Internet, but also the other information systems that support our businesses, infrastructure and services." The strategy illustrates the critical infrastructure which is necessary for society's everyday activities.

According to the U.S. viewpoint "Cyberspace is their [critical infrastructures] nervous system — the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security." The definition highlights the critical infrastructure rather than network services, information contents or service users.

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 (Grobler et al., 2011). Some researchers also include societal and infrastructure domains in cyberspace. Nonetheless, the Internet is an integral and elemental part of this new world.

South African researchers have created a model of cyberspace's most important structures. These are the economy, politics, the armed forces, psychology and information. According to this model economic structures are a significant target for cyber threats. Political structures are responsible for maintaining national security and the viability of an open society. The armed forces are tasked to maintain national security and to protect society against the measures of cyberwar. The psychological dimension plays an important role in the cyber world; psychological operations can influence human thinking and behaviour. The revolutions in North Africa demonstrated the influence of the media on people's opinions. Information plays the most important part in each cyber threat situation. The western information societies are dependent on the existence, credibility and availability of information (Ibid).

Professor Martin C. Libicki has created a structure for the cyber world, whose idea is based on the Open Systems Interconnection Reference Model (OSI). The OSI model groups communication protocols into seven layers. Each layer serves the layer above it and is served by the layer

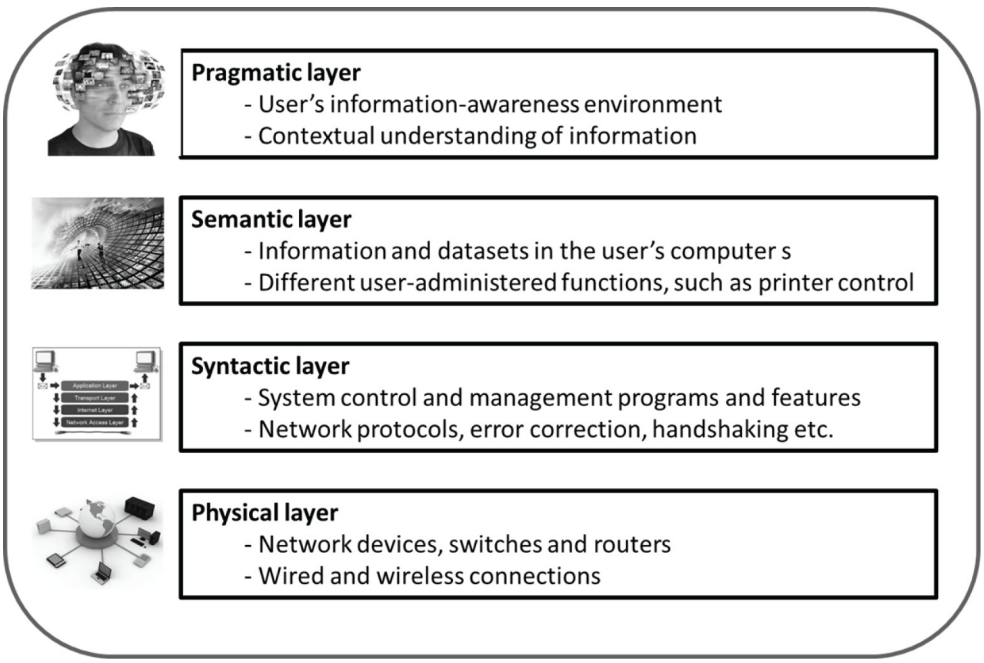
below it. The Libicki cyber world model has the following four layers: physical, syntactic, semantic and pragmatic, as seen in Figure 1. The physical layer contains the physical elements of the communications network, such as network devices, switches and routers as well as wired and wireless connections. The syntactic layer is formed of various system control and management programs and features which facilitate interaction between the devices connected to the network, such as network protocols, error correction, handshaking, etc. Libicki believes that the semantic layer is the heart of the entire network. It contains the information and datasets in the user's computer terminals as well as different user-administered functions, such as printer control. The pragmatic layer portrays the user's information-awareness environment: a world in which information is being interpreted and where one's contextual understanding of information is created (Libicki, 2007).

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, 2011) uses the term to describe the "systems and services connected either directly to or indirectly to the internet, telecommunications and computer networks." The International Organisation for Standardisation (ISO, 2012) 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."

The US Joint Publication 3-13 (Information Operations 2012) 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."

The global cyberspace comprises a complex and multilayered IT network which encompasses ICT networks operated by na-

Figure 1. Shows the Libicki four-layer model



tional government authorities, the business community and security authorities, as well as monitoring and control systems for the industry and critical infrastructure. Through the Internet, they connect to a world-wide network. Users connect to this global network through different intelligent data terminal equipment.

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.

2. CYBER THREATS, VULNERABILITIES AND WEAPONRY

2.1. Classification of the Cyber Threats

The global community continues to experience an increase in the scale, sophistication and successful perpetration of cyber-attacks. As the quantity and value of electronic information has increased so too have the efforts of criminals and other malicious actors who have embraced the Internet as a more anonymous, convenient and profitable way of carrying out their activities. Of primary concern is the threat of organized cyber-attacks capable of causing debilitating disruption to a nation's critical infrastructures, functions vital to society, economy, or national security.

Threats in cyberspace are difficult to define as it is hard to identify the source of attacks and the motives that drive them, or even to foresee the course of an attack as it unfolds. The identification of cyber threats is further complicated by the difficulty in defining the boundaries between national, international, public and private interests. Because threats in cyberspace are global in nature and involve rapid technological developments, the struggle to meet them is ever-changing and increasingly complicated.

Threats to society's vital functions may directly or indirectly target national systems and/or citizens, from within or outside the national borders. The threats to society's vital functions can be divided into three entities which are: physical threats, economic threats and cyber threats.

Physical threats include:

- Natural disasters (e.g. earthquake, tsunami, volcanic eruption, flood);
- Environmental disasters (e.g. nuclear fall-out, oil spill, toxic chemical discharges);
- Widespread technical disruptions (especially those in ITC systems);
- Conventional warfare with kinetic weapon systems;
- Terrorist strikes with kinetic weapon systems;
- Civil unrest (violence, sabotage).

Economic threats include:

- Deep national depression;
- Deep global depression;
- Disruption in national or global financing markets;
- Sudden global shortage of goods and services.

Threats in cyberspace are difficult to define as it is hard to identify the source of attacks and the motives that drive them, or even to foresee the course of an attack as it unfolds. The identification of cyber threats is further complicated by the difficulty in defining the boundaries between national, international, public and private interests. Because threats in cyberspace are global in nature and involve rapid technological developments, the struggle to meet them is ever-changing and increasingly complicated.

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 weak-

nesses/vulnerabilities, threats may lead to a loss or takeover of assets (ENISA 2012b).

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 (ENISA, 2012b).

One of the common threat models is a fivefold classification based on motivational factors: cyber activism, cybercrime, cyber espionage, cyber terrorism and cyber warfare. With a typology such as this motives can reduced to their very essence: egoism, anarchy, money, destruction and power. This fivefold model is derived from Myriam Dunn Cavelty's structural model as depicted in Figure 2 (Dunn Cavelty, 2010; Ashenden, 2011).

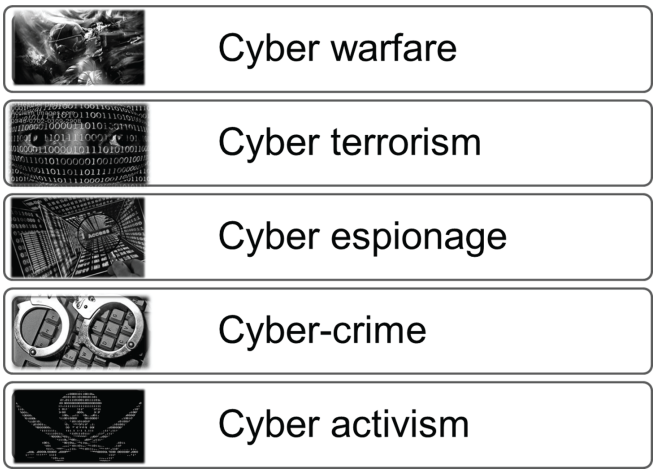
Level 1 consists of cyber activism which encompasses cyber vandalism, hacking and hacktivism. For a single company or an individual their activities can cause significant economic losses. The recent activities of the Anonymous hackers have been more effective than in the past.

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" (Commission of the European Communities 2007). According to the Commission, cybercrime can be divided into three categories of criminal activities:

1. Traditional forms of crime committed over electronic communication networks and information systems, such as harassment, threats or fraud;
2. The publication of illegal content over electronic media, e.g. child sexual abuse material or incitement to racial hatred;
3. Crimes unique to electronic networks, e.g. network attacks, denial-of-service attacks and hacking.

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

Figure 2. The structure of cyber threats



the Internet, networks, programs or computers (Liaropoulos, 2010).

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 (Beggs, 2006).

Level 5 cyber warfare consists of three separate entities: strategic cyber warfare, tactical/operational cyber warfare and cyber warfare in low-intensity conflicts. No 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. The Russo-Georgian war in August 2008 was a good example of this. On 8 August 2008 several Georgian and South-Ossetian web pages were the targets of denial of service-attacks. The web pages of Russian news services RIA Novosti and Russia Today were attacked and they crashed for a few hours on 10 August.

In the spring of 2007 Estonia became the victim of a series of network attacks for a period of three weeks. The targets included, among others, state leadership, the police, the banking establishment, the media and the business community. The operation mostly used denial of service-attacks targeted at web servers, e-mail servers, DNS-servers and routers. According to the Estonians, this attack cannot be considered as genuine cyber warfare, but rather was regarded as a cyber conflict (Ottis, 2008).

Figure 2 contains an illustration of the cyber threats used in this paper.

The threats to society's vital functions can also simultaneously occur in each of the three above mentioned dimensions. For example, cyber operations and action aimed at collapsing an adversary's economy can be included in conventional warfare. When it comes to terrorism, different operations in the cyber world and the economic system can be included in strikes that cause physical destruction.

Disruptions can impact and escalate across the dimensions. For instance, a natural disaster can cause widespread disruptions in the power grid, which may adversely affect the operation of payment systems and the food distribution chain. When prolonged, they may result in civil disturbances.

2.2. 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, organisational solutions (management, security processes, methods and procedures and the security culture) and security technology solutions.

According to the ISO 27005 definition, risks emerge from the "potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization". The risk depends on:

- The *Asset* covering its business importance, existing vulnerabilities or weaknesses and level of protection implemented through controls;
- The *Threat* consisting of a threat agent who – depending on their capabilities - utilizes an attack vector to compromise an asset or set of assets. The effectiveness of an attack

depends on the capability of the threat agent and the sophistication of the attack;
- The *Impact* that takes into account the value that the asset represents for the business and the consequences when the confidentiality, integrity, availability or privacy of that asset is compromised though the threat (ENISA 2012b).

Figure 3 shows the interaction between threats, vulnerabilities, risks and countermeasures as per the ISO 15408:2005 standard (ENISA, 2012b).

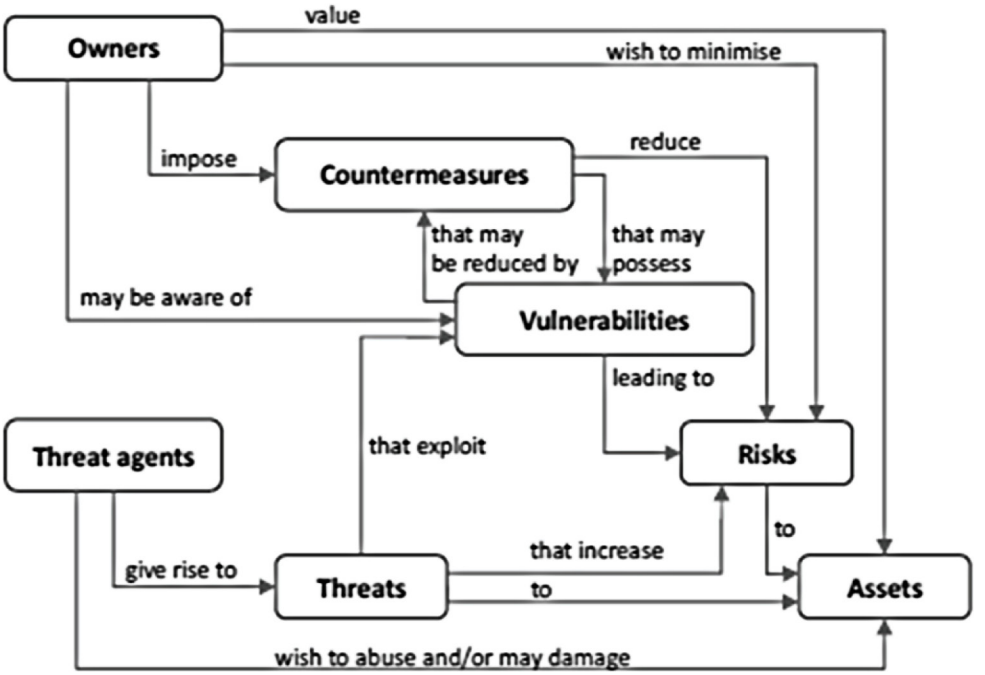
2.3. Cyber Weaponry

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. Malware is hardware, software, or firmware that is intentionally included or inserted in a system for a harmful purpose (Internet Security Glossary, RFC 2828). 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 (Kiravuo et al., 2013).

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 (Ibid).

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

Figure 3. Interaction model for cyber threats, cyber vulnerabilities, cyber risks and countermeasures



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 (Ibid).

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 (Ibid).

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 (Ibid).

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 (Ibid).

Then the delivery vehicle, constructed of the above mentioned 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. (Ibid) Figure 4 illustrates the design of a standard cyber weapon.

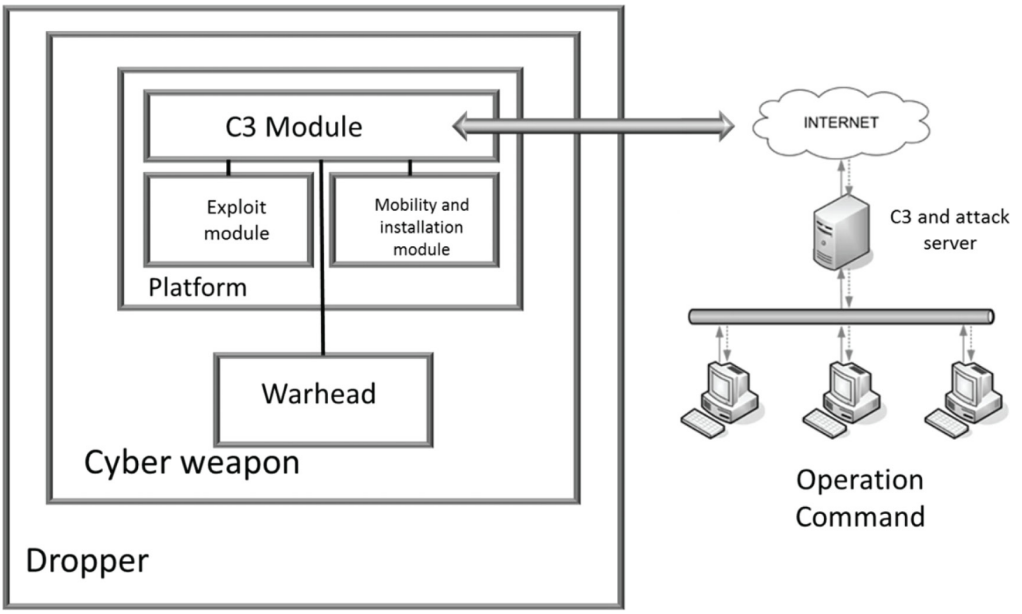
In other words cyber weapons comprise a group of extremely sophisticated computer programs whose functionality determines their targets. Cyber weaponry is used in cyber operations whose aim is to create a desired effect in the target through malware. Typical cyber weapons include (DCSINT Handbook No. 1.02, 2005):

- Adware;
- Backdoor;
- Root-kit;
- Scareware;
- Sniffer;
- Spyware;
- Trojan Horse;
- Logic Bomb;
- Time Bomb;
- Viruses;
- Worms;
- Zombie.

ENISA (2012b) uses a cyber threat landscape model, consisting of threat scenarios. These scenarios include attack methods and techniques, malware and physical threats. The attack methods and techniques include the following:

- Abuse of Information Leakage;
- Code Injection Attacks;
- Compromising confidential information;
- Botnets;
- Denial of Service Attacks (DOS);
- Distributed denial of service attack (DDOS);
- Drive-by Exploits;
- E-mail Spoofing;
- Identity Theft;
- IP Address Spoofing;

Figure 4. A standard cyber weapon



- Keystore Logging;
- Password Cracking;
- Phishing;
- Search Engine Poisoning;
- Spamming;
- Targeted Attacks.

By merging the attack methods and techniques with the Libicki four-layer model one gets the synopsis illustrated in Figure 5.

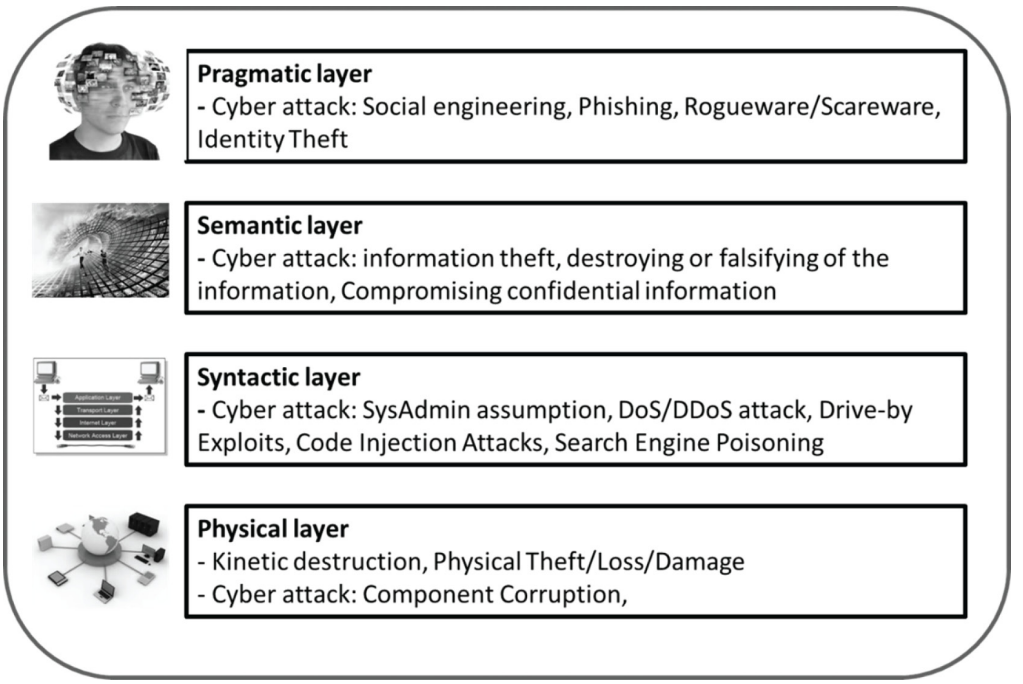
3. CYBER THREATS IN THE CYBER SECURITY STRATEGIES

Australia's cyber security strategy identifies cybercrime as the primary cyber treat. "The global community continues to experience an increase in the scale, sophistication and successful perpetration of cybercrime. Just as we have seen the benefits of ICT in promoting legitimate economic activity, we now see cybercrime emerging on an unprecedented scale." In addition, the strategy refers to the National Security Statement, published in 2008, which states that "Electronic espionage, both commercial and state-based, will be a growing vulnerability as the Australian Government and society become more dependent on integrated information technologies."

Canada's cyber security strategy includes a chapter dedicated to cyber threats. The strategy identifies three types of threats. Cyber Crime: Once they have access to a computer, attackers can steal or distort the information stored on it, corrupt its operations and program it to attack other computers and the systems to which they are connected. Cyber Espionage: The most sophisticated cyber threats come from the intelligence and military services of foreign states. Cyber terrorism: Terrorist networks also are moving to incorporate cyber operations into their strategic doctrines. Among many activities, they are using the Internet to support their recruitment, fundraising and propaganda activities.

The cyber security strategy of the Czech Republic provides a brief description of cyber-attacks. In accordance with the strategy "such attacks may be a new type of warfare, or may

Figure 5. Attack methods into the different layers of the cyber world



have a criminal, economic, or terroristic motive and be launched to destabilize the society. The nature and motives of the attackers also change." Consequently, the strategy lists cybercrime, cyber terrorism and cyber warfare as motives.

The Estonian cyber security strategy presents a three-tier cyber threat model. Its motivational factors encompass cybercrime, cyber terrorism and cyber warfare. Moreover, the strategy states that "advanced technologies and attack methods make it difficult to define with any certitude or clarity the motives impulsing an attack, threats can also be classified on the basis of methods employed and on the extent of damage inflicted."

Finland's cyber security strategy does not explicitly describe the threat. It only states that "threats against the cyber domain have increasingly serious repercussions for individuals, businesses and society in general. The perpetrators are more professional than before and today the threats even include state actors. Cyber-attacks can be used as a means of political and economic pressure; in a serious crisis pressure can be exerted as an instrument of influence alongside traditional means of military force."

When it comes to defining cyber threat, Germany's cyber security strategy parallels that of Finland, focusing on the cyber-attack. "Given the openness and extent of cyberspace it is possible to conduct covert attacks and misuse vulnerable systems as tools for an attack. In view of technologically sophisticated malware the possibilities of responding to and retracing an attack are rather limited. Often attacks give no clue as to the identity and the background of the attacker." In addition, the strategy lists actors that may commit the attacks: "Criminals, terrorists and spies use cyberspace as a place for their activities and do not stop at state borders. Military operations can also be behind such attacks."

The Netherlands' cyber security strategy also concentrates on a description of cyber-attacks. "When cyber-attacks occur, it is often difficult to identify the perpetrator, who may be

a loner, an organization, a state, or a combination of all three. The nature of the cyber threat is also often unclear. But many cyber-attacks involve the same techniques and methods – illustrating the importance of further cooperation among parties concerned with cyber security, including public bodies working on particular types of threat, businesses that maintain the network and information infrastructure, and knowledge institutions concerned with cyber security and the public."

The cyber security strategy of the United Kingdom lists three threat agents: criminals, spies and terrorists. The strategy states that "criminals from all corners of the globe are already exploiting the internet to target the UK in a variety of ways. Some of the most sophisticated threats to the UK in cyberspace come from other states which seek to conduct espionage with the aim of spying on or compromising our government, military, industrial and economic assets, as well as monitoring opponents of their own regimes. Cyberspace is already used by terrorists to spread propaganda, radicalise potential supporters, raise funds, communicate and plan. While terrorists can be expected to continue to favour high-profile physical attacks, the threat that they might also use cyberspace to facilitate or to mount attacks against the UK is growing."

In turn, the U.S. cyber security strategy describes cyber-attacks as follows: "a spectrum of malicious actors can and do conduct attacks against our critical information infrastructures. Of primary concern is the threat of organized cyber-attacks capable of causing debilitating disruption to our Nation's critical infrastructures, economy, or national security. Cyber-attacks on U.S. information networks can have serious consequences such as disrupting critical operations, causing loss of revenue and intellectual property, or loss of life."

Cyber security strategies discuss cyber threats, vulnerabilities and the different forms of cyber conflict in a varying manner. Attacks against a country's critical infrastructure and ICT infrastructure are considered to be the most important threats. As states are increasingly reliant on networked structures, these targets are regarded vital to the functioning of society. Digital control systems (Supervisory Control and Data Acquisition, SCADA) that manage the electric grid and water supply are the key systems of society's critical functions. When their controls changed over to modern network-based systems their vulnerabilities increased. Consequently, this increased the threat of an attack. The strategies do not discuss cyber warfare; it is only mentioned in the strategies of the Czech Republic, Estonia and the United States.

Cybercrime is felt to be constantly increasing. In particular, in the Internet world cybercrime causes enormous financial losses to individuals and companies on a global scale. The key security measures in the Internet environment are predominantly associated with the prevention of cybercrime.

Cyber espionage is the third most important threat. The targets of cyber espionage include the central government, armed forces, weapons industry and the business community in general as well as the academia. According to observations, cyber espionage amounts to a terabyte's worth of stolen information on an annual level.

Most strategies mention cyber terrorism. It is not perceived as a separate entity, instead it is regarded as a functional area of terrorism. Nor is it described from the traditional viewpoint of the concept of terrorism. The Internet plays a significant role in cyber terrorism due to the fact that terrorist organizations can promulgate information over the Internet or recruit and train new members.

Table 1 presents the prevalence of cyber threats in the strategies that were studied for this paper.

4. KEY OBJECTIVES AND FOCUS IN CYBER SECURITY STRATEGIES

Cyber Security Strategies define a roadmap for the implementation of the strategy. It contains concrete activities that would meet the objectives of the strategy and a governance

Table 1. Cyber threats in the cyber security strategies

Country	Cyber Activism	Cyber Crime	Cyber Espionage	Cyber Terrorism	Cyber Warfare
Australia	x	x	x	x	
Canada		x	x	x	
Czech Republic		x		x	x
Estonia		x		x	x
Finland		x			
Germany		x	x	x	
Netherlands	x	x	x	x	
United Kingdom	x	x	x	x	
United States of America	x	x	x	x	x

framework for the implementation, evaluation and maintenance of the strategy. The cyber security strategy also has a master plan for the implementation of the strategy and a concrete action plans for each activity.

The Australian cyber security strategy (2009) clearly identifies the aims and the objectives of the cyber security policy. The citizens are put first in the Australian cyber security's objectives: "All Australians are aware of cyber risks, secure their computers and take steps to protect their identities, privacy and finances online." Next, the strategy's security measures focus on the business community, which "operates secure and resilient information and communications technologies to protect the integrity of their own operations and the identity and privacy of their customers." Third, "the Australian Government ensures its information and communications technologies are secure and resilient." The strategy lists 7 strategic priorities:

1. Improve the detection, analysis, mitigation and response to sophisticated cyber threats;
2. Educate and empower all Australians with the information, confidence and practical tools to protect themselves online;
3. Partner with business to promote security and resilience in infrastructure, networks, products and services;
4. Model best practice in the protection of government ICT systems;
5. Promote a secure, resilient and trusted global electronic operating environment;
6. Maintain an effective legal framework and enforcement capabilities to target and prosecute cyber-crime;
7. Promote the development of a skilled cyber security workforce with access to research and development to develop innovative solutions.

Canada's Cyber Security Strategy prioritizes the objectives and aims in the opposite manner. "The Strategy (2010) is built on three pillars: [1] Securing Government systems, [2] Partnering to secure vital cyber systems outside the federal Government, and [3] Helping Canadians to be secure online. Canada's Cyber Security Strategy will strengthen the cyber systems and critical infrastructure sectors, support economic growth and protect Canadians as they connect to each other and to the world."

1. Securing Government Systems contains the following priorities:
   a. Establishing Clear Federal Roles and Responsibilities;
   b. Strengthening the Security of Federal Cyber Systems;

   c. Enhancing Cyber Security Awareness throughout Government;
2. Partnering to Secure Vital Cyber Systems focuses on the following key areas:
   a. Partnering with the Provinces and Territories;
   b. Partnering with the Private Sector and Critical Infrastructure Sectors;
3. Helping Canadians to be Secure Online has two priorities:
   a. Combatting Cybercrime;
   b. Protecting Canadians Online.

The Cyber Security Strategy of the Czech Republic (2011) does not itemize the objectives. Rather, it generally states that "it defines interests and intentions of the Czech Republic in the field of cyber security needed to build up a credible information society with solid legal foundations, which is committed to a secure cyber transmission and processing of information in all domains of human activities and makes sure that the information can be used and shared freely and safely." The Strategic objectives are:

1. Legislative framework;
2. Strengthening of cyber security of the public administration and CI ITCs;
3. Establishment of a national CERT agency;
4. International cooperation, cooperation of the state, private sector and academia;
5. Increased cyber security awareness.

Estonia's cyber security strategy (2008) seeks primarily to reduce the inherent vulnerabilities of cyberspace in the nation as a whole. "Estonia's cyber security should be pursued through the coordinated efforts of all concerned stakeholders, of public and private sectors as well as of civil society." The Estonian cyber security strategy lists 5 strategic goals which also describe the measures used in achieving the goals. The cyber security goals are:

1. Development and implementation of a system of security measures;
2. Increasing competence in information security;
3. Development of a legal framework for cyber security;
4. Development of international co-operation;
5. Raising awareness of cyber security.

There are three visions for cyber security in Finland's cyber security strategy (2013). The first one states: "Finland can secure its vital functions against cyber threats in all situations." The next vision is that "citizens, the authorities and businesses, can effectively utilise a safe cyber domain and the competence arising from cyber security measures, both nationally and internationally." The third vision, as per the Finnish Government Programme, is that "by 2016, Finland will be a global forerunner in cyber threat preparedness, and in managing the disturbances caused by these threats." The strategy lists the following 10 strategic guidelines:

1. Create an efficient collaborative model between the authorities and other actors;
2. Improve comprehensive cyber security situation awareness among the key actors;
3. Maintain and improve the ability to detect and repel cyber threats and disturbances;
4. Ensure the police have sufficient capabilities to prevent, expose and solve cybercrime;
5. The Finnish Defence Forces will create a comprehensive cyber defence capability;
6. Strengthen cyber security through active and efficient participation in the activities of international organizations;
7. Improve the cyber expertise and awareness of all societal actors;
8. Provide national legislation for effective cyber security measures;
9. Assign cyber security related tasks to the authorities and actors in the business community;
10. Monitor the implementation of the Strategy and its completion.

The Cyber Security Strategy for Germany (2011) states that "the Federal Government aims at making a substantial contribution to a secure cyberspace, thus maintaining and promoting economic and social prosperity in Germany. Cyber security in Germany must be ensured at a level commensurate with the importance and protection required by interlinked information infrastructures, without hampering the opportunities and the utilization of the cyberspace." The strategy identifies the following 10 strategic areas:

1. Protection of critical information infrastructures;
2. Secure IT systems in Germany;
3. Strengthening IT security in the public administration;
4. National Cyber Response Centre;
5. National Cyber Security Council;
6. Effective crime control also in cyberspace;
7. Effective coordinated action to ensure cyber security in Europe and worldwide;
8. Use of reliable and trustworthy information technology;
9. Personnel development in federal authorities;
10. Tools to respond to cyber attacks.

According to the cyber security strategy of the Netherlands (2011) the "goal is to strengthen the security of digital society in order to give individuals, businesses, and public bodies more confidence in the use of ICT. To this end, the responsible public bodies will work more effectively with other parties to ensure the safety and reliability of an open and free digital society." The strategy lists the following 6 priority activities:

1. Setting up the Cyber Security Council and the National Cyber Security Centre;
2. Setting up threat and risk analyses;
3. Increasing the resilience of critical infrastructure;
4. Capacity for responding to ICT disruptions and cyber attacks;
5. Intensifying the investigation of cybercrime and the prosecution of its perpetrators;
6. Encouraging research and education.

The vision in the UK cyber security strategy is "for the UK in 2015 to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society. Achieving this vision will require everybody, the private sector, individuals and government, to work together." The strategy lists the following 4 objectives for the purpose of achieving the vision:

1. The UK to tackle cyber crime and be one of the most secure places in the world to do business in cyberspace;
2. The UK to be more resilient to cyber attacks and better able to protect our interests in cyberspace;
3. The UK to have helped shape an open, stable and vibrant cyberspace, which the UK public can use safely and that supports open societies;
4. The UK to have the cross-cutting knowledge, skills and capability it needs to underpin all our cyber security objectives.

The policy of the U.S. cyber security strategy (2003) is "to prevent or minimize disruptions to critical information infrastructures and thereby protect the people, the economy, the essential human and government services, and the national security of the United States." The Strategy articulates five national priorities. The first priority focuses on improving the ability to respond to cyber incidents and reduce the potential damage from such events. The second, third, and fourth priorities aim to reduce the numbers of cyber threats and overall vulnerability to cyber-attacks. The fifth priority focuses on preventing cyber-attacks with the potential to impact national security assets and improving international management of and response to such attacks.

Of all of the strategies researched six key priorities could be identified which appeared in almost every cyber security strategy. These priority areas are:

1. Roles and responsibilities of cyber security;
2. Cyber security center / situation awareness;
3. Legislation and supervising the lawfulness of government actions;
4. Cyber security training and research;
5. Secure ICT products and services;
6. National and international cooperation.

A number of various proposals for action were presented within the scope of these priority areas. The number of said proposals varied from 7 to 57, and there were marked differences as regards their level of detail. The bulk of the proposals related to various public sector-associated initiatives. The strategies do not attach these initiatives to any administrative branch, in other words, the strategies only present a number of different measures without assigning responsibilities to any organisation. Only the U.S. strategy lists the actors responsible for the different segments of critical infrastructure.

When it comes to cyber security management and responsibilities, the strategies present quite divergent approaches. Whereas the German strategy proposes the establishment of a National Cyber Security Council, the Finnish strategy states that "Each ministry is in its sector responsible for preparing cyber security related matters and appropriate arrangement of administrative matters". Many other strategies only make passing reference to the management of cyber security and the responsibilities of each actor.

Table 2 presents the most prevalent objectives and priorities in the cyber security strategies of different countries.

Table 2. Cyber strategy objectives and priorities

Country	Roles and Responsibilities of Cyber Security	Cyber Security Center/ Situation Awareness	Legislation and Supervising the Lawfulness of Government Actions	Cyber Security Training and Research	Secure ICT Products and Services	National and International Cooperation
Australia		x	x	x	x	x
Canada	x	x	x	x	x	
Czech Republic	(x)	x	x	x	x	x
Estonia	x	x	x	x	x	x
Finland	x	x	x	x		x
Germany	x	x	x	x	x	x
Netherlands	x	x	x	x	x	x
United Kingdom	x	x	x	x	x	x
United States of America	x	x	x	x	x	x

5. SUMMARY

This paper analyzed nine cyber security strategies. All of the strategies presented a focus, the cyber threat (at least in general terms), and strategic objectives. Yet, significant variance was to be found in their scope and depth.

The cyber security strategy lays the foundation for society's preparedness. The strategies present a threat scenario which is a general illustration of possible disruptions in the security environment. The threats, originating from within or outside the national borders, may directly or indirectly impact society's vital functions, national critical infrastructure and/or citizens.

The strategies' cyber threat scenarios represent a classification based on the actors' motives and the form in which the threat materializes, and its impact. Cyber security strategies varyingly address the different forms of cyber threats, vulnerabilities and cyber conflicts. Different attacks against the nation's critical infrastructure and critical information infrastructure are considered to be the most serious threat. The next biggest threats include cybercrime and cyber espionage. While most strategies do mention cyber terrorism, it is perceived to be but one form of terrorism, rather than an individual function. Some strategies give mention to cyber warfare. However, no extensive analysis is given.

The global cyberspace connects states, businesses and citizens in an entirely new manner. The significance of time and place in communications has transformed. Although the digital information society has remarkably increased well-being, on the flip side it also contains risks of various cyberspace threats. It is much faster and cheaper to move and operate in cyberspace compared to land, sea or air. The target of an attack can be inexpensively reached from anywhere in the world, and the command servers that execute the operation can be positioned in any country, cloaking the actual perpetrator of the attack.

The new arrangement alters traditional international power positions. This situation provides even small states or non-state operators effective means of operation in cyberspace. When it comes to cyberspace, size or mass no longer matter. Competence matters. The great powers have significant resources available for cyberspace activities; however, they do not completely dominate it. Small actors can acquire sufficient skills and resources through which they are able to take advantage of vulnerabilities in cyberspace. Small actors are not only states; they also include non-profit organizations as well as ethnic, religious and criminal groups.

The actors in cyberspace that possess sufficient technological savvy and resources can execute cyber-attacks from any distance. Cyber-attacks can generate massive disruptions and even paralyze critical infrastructure and society's vital functions.

The creation and development of a national cyber security strategy requires close cooperation between all stakeholders. While many different definitions of cyber security exist, it is generally considered to be an instrument that helps governments manage security measures in controlling cyber security risks, and creates the kind of cyber resilience that serves the national goals.

REFERENCES

Ashenden, D. (2011). Cyber security: Time for engagement and debate. In *Proceedings of the 10th ECIW Conference*, Tallinn, Estonia (pp. 15).

Australian cyber security strategy. (2009).

Beggs, C. (2006). Proposed risk minimization measures for cyber-terrorism and SCADA networks in Australia. In *Proceedings of the 5th ECIW Conference*, Helsinki, Finland (pp. 9-18).

Canada's cyber security strategy. (2010).

Czech Republic Cyber Security Strategy. (2011). *DCSINT handbook No. 1.02: Cyber operations and cyber terrorism*. (2005).

Dunn Cavelty, M. (2010). *The reality and future of cyber war*. Parliamentary Brief.

ENISA. (2012a). National cyber security strategies. *Practical guide on development and execution*.

ENISA. (2012b). *Threat landscape, responding to the evolving threat environment*.

Estonia cyber security strategy. (2008).

Finland´s cyber security strategy. (2013).

Germany cyber security strategy. (2011).

Gibson, W. (1984). *Neuromancer*. New York, NY: The Berkley Publishing Group.

Grobler, M., van Vuuren, J. J., & Zaaiman, J. (n.d.). Evaluating cyber security awareness in South Africa. In *Proceedings of the 10th ECIW Conference*, Tallinn, Estonia (pp. 114-115).

Internet Security Glossary (RFC 2828). (2000).

ISO. (2005). [Information technology - Security techniques - Evaluation criteria for IT security.]. *IEC*, *15408*, 2005.

ITU. (2011). *ITU national cybersecurity strategy guide*. Geneva.

Kiravuo, T., Särelä, M. J. M. J. (2013). *Aalto-yliopisto, Kybersodan taistelukentät, Sotilasaikakauslehti 3/2013.*

Kuusisto, R. (2012). KYBER – miten se voitaisiinkaan määritellä? lecture 10.10.2012. Helsinki.

Liaropoulos, A. (2010). War and ethics in cyberspace: Cyber-conflict and just war theory. In *Proceedings of the 9th ECIW Conference*, Thessaloniki, Greece (pp. 177-182).

Libicki, M. C. (2007). *Conquest in cyberspace – National security and information warfare*. Cambridge University Press. doi:10.1017/CBO9780511804250

NATO CCD COE. (2012). *National cyber security framework manual*.

Porter, A. (1969). *Cybernetics simplified*. London, UK: English University Press.

Rain, O. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. In *Proceedings of the 7th European Conference on Information Warfare and Security,* University of Plymouth, UK.

Ståhle, P. (2004). *Itseuudistumisen dynamiikka - systeemiajattelu kehitysprosessien ymmärtämisen perustana, verkkodokumentti*.

The National cyber security strategy. (2011). Netherlands.

The national strategy to secure cyberspace. (2003). United States of America. *UK cyber security strategy*. (2011).

US Joint Publication 3-13 (Information Operations 2012). (2012).