THESIS ON INFORMATICS AND SYSTEM ENGINEERING C60

A Systematic Approach to Offensive Volunteer Cyber Militia

RAIN OTTIS

TUT
PRESS

Faculty of Information Technology
Department of Informatics
Chair of Information Security
TALLINN UNIVERSITY OF TECHNOLOGY

Dissertation was accepted for the defense of the degree of Doctor of Philosophy in Engineering on April 06, 2011.

Supervisor: Prof. Dr. Peeter Lorents. Research and Development Branch Chief, Cooperative Cyber Defence Centre of Excellence

Prof. Dr. Ahto Buldas. Chair of Information Security, Department of Informatics, Faculty of Information Technology, Tallinn University of Technology

Opponents: Dr. Gabriel Jakobson. Altusys Corporation, USA

Prof. Dr. Leo Mõtus. Chair of Real-time Systems, Department of Computer Control, Faculty of Information Technology, Tallinn University of Technology

Defense of the thesis: May 06, 2011

Declaration
Hereby I declare that this doctoral thesis, my original investigation and achievement, submitted for the doctoral degree at Tallinn University of Technology has not been submitted for any academic degree or examination at any other university.

/ Rain Ottis /

ISSN 1406-4731
ISBN 978-9949-23-073-0 (publication)
ISBN 978-9949-23-074-7 (PDF)

INFORMAATIKA JA SÜSTEEMITEHNIKA C60

Vabatahtlikud küberründegrupid: süsteemiteoreetiline vaade

RAIN OTTIS

TTÜ
KIRJASTUS

Table of Contents

Introduction 7
Research questions 7
Publications 8
Overview 8
The nature of the topic 9
Acknowledgements 9
1. Related work 10
1.1 Military art and science 10
1.2 The Law of Armed Conflict 12
1.3 Information operations 13
1.4 Cyber security and national security 14
1.5 Cyber forces and volunteer cyber militia 14
2. The systematic approach 16
2.1 Why systematic approach? 16
2.2 Knowledge, Data and Information 17
2.3 Systems and the systematic approach 18
2.4 Security of Information 19
2.4.1 Availability of Information 20
2.4.2 Integrity of Information 20
2.4.3 Confidentiality of Information 21
2.5 Application of the systematic approach 21
3. Key concepts in cyber conflict 22
3.1 Information technology and cyber weapons 22
3.2 Cyber incidents, attacks, conflicts and war 23
4.3 Cyberspace and cyber society 24
4. Offensive volunteer cyber militia 25
4.1 Method and limitations 25
4.2 The Forum 25
4.2.1 Attributes 26
4.2.2 Strengths 27
4.2.3 Weaknesses 28
4.3 The Cell 28
4.3.1 Attributes 29
4.3.2 Strengths 30
4.3.3 Weaknesses 30
4.4 The Hierarchy 31
4.4.1 Attributes 31
4.4.2 Strengths 32
4.4.3 Weaknesses 32
4.5 Comparison 33
5. Defending against volunteers 34

5.1 On-line cyber militia 34
5.2 Neutralizing an on-line cyber militia 35
5.2.1 Attacking plans 36
5.2.2 Attacking alliances 36
5.2.3 Attacking the army 37
5.2.4 Attacking fortified cities. 37
Summary 38
Future research 38
KOKKUVÕTE 39
ABSTRACT 40
References 41
ELULOOKIRJELDUS 48
CURRICULUM VITAE 51
Publications 55

Introduction

Over the course of 22 days in April and May of 2007, Estonia was subject to an offensive cyber campaign. Among the targets were government, finance sector, media and many other systems. Following the attacks, the prevailing wisdom seems to be that it was the work of hactivists (short for hacker activists) who were supportive of the Russian Government's policy (CCDCOE 2009).

While, in general, Estonia was successful in dealing with the attacks, the situation was clearly problematic for the stability of the nation and an example of a larger trend in cyber security (Czosseck, Ottis & Talihärm 2011; Nazario 2009). Politically motivated hactivism campaigns have grown from a mere nuisance of the 1990's to a potential national security threat of today.

At the time of the Estonia campaign I was in charge of the Cyber Defence section at the Estonian Defence Forces Training and Development Centre of Communication and Information Systems (EDF TDCCIS). My responsibilities included cyber defense awareness, training and analysis projects in the Defence Forces. I was therefore fortunate to participate in the Ministry of Defence led analysis, which gave me interesting insight into the problem of malicious volunteer actors in cyber conflicts (from the defender's perspective). I started my PhD studies a few months after the attacks, determined to look into this issue in depth and to identify solutions that would help deal with this threat. Events, such as the ones in Georgia in 2008 and in Israel and Gaza in 2009 have proven that the problem is relevant to a wider community of interest.

It should be noted that the line of research presented in this thesis should not to be considered as the views or policy of Tallinn University of Technology, the Estonian Defence Forces, the Cooperative Cyber Defence Centre of Excellence or the North Atlantic Treaty Organization.

Research questions

Inspired from the cyber attack campaign against Estonia in 2007, I started to study the issue of politically motivated cyber attacks by non-state actors, especially the ones that may rise to the level of a national security threat. I quickly discovered that the field was not well covered and contained numerous ambiguous interpretations even in terms of key concepts, such as the notion of cyber attack or cyber weapon. In an effort to specify my search, I settled with the following research questions:

a. How to define the key concepts in cyber conflict as part of a well founded system of definitions?
b. How to describe the attributes, strengths and weaknesses of volunteer cyber militia groups in a systematic way?
c. How can the threat from loosely connected volunteer cyber militias be neutralized?

Question (a) is addressed in Chapter 3, question (b) in Chapter 4 and question (c) in Chapter 5.

Publications

The main contribution of this thesis is based on the publications listed below and referred to in the text using the corresponding Roman number, in bold face. I am the sole contributor to (**II;III;VI**). In (**I**), my contributions are primarily the definitions of cyber incident, attack, weapon, conflict, espionage and war. The contribution to definitions in (**IV;V**) is divided equally between me and Lorents. The publications are the basis for my contribution in Chapter 3 (**I;IV;V**), 4 (**II;III;VI**) and 5 (**III**). In addition, the thesis also includes references to my other publications, which are listed in the references section (see Czosseck, Ottis & Talihärm 2011; Ottis 2008, 2009, 2010).

I Lorents, P. and Ottis, R. (2010) Knowledge Based Framework for Cyber Weapons and Conflict. In Czosseck, C. and Podins, K. (Eds.) *Conference on Cyber Conflict. Proceedings 2010*. Tallinn: CCD COE Publications, p 129-142.

II Ottis, R. (2011) Theoretical Offensive Cyber Militia Models. In *Proceedings of the 6th International Conference on Information Warfare and Security*, Washington DC. Reading: Academic Publishing Limited, p 307-313.

III Ottis, R. (2010) Proactive Defence Tactics Against On-Line Cyber Militia. In *Proceedings of the 9th European Conference on Information Warfare and Security*, Thessaloniki. Reading: Academic Publishing Limited, p 233-237.

IV Ottis, R., Lorents, P. (2010) Cyberspace: Definition and Implications. In *Proceedings of the 5th International Conference on Information Warfare and Security*, Dayton, OH, US, 8-9 April. Reading: Academic Publishing Limited, p 267-270.

V Lorents, P., Ottis, R., Rikk, R. (2009). Cyber Society and Cooperative Cyber Defence. In *Internationalization, Design and Global Development*. *Lecture Notes in Computer Science*, Vol 5623, p 180-186.

VI Ottis, R. (2009) Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability. In *Proceedings of the 8th European Conference on Information Warfare and Security, Lisbon*. Reading: Academic Publishing Limited, p 177-182.

Overview

Chapter 1 gives a brief overview of related work in relevant fields of research. Chapter 2 (method) explains the systematic and knowledge based approach. It covers concepts like knowledge, data, information, confidentiality, integrity, availability, destruction of information, system, as well as the idea of life and death of systems. Chapter 3 introduces my contribution to defining key concepts in cyber conflict research, such as cyber weapon, cyber attack, cyber conflict and cyber warfare. Chapter 4 describes the properties, strengths and weaknesses of three generic types of cyber militia and describes them as

systems. Chapter 5 provides possible alternative solutions for dealing with the threat from loosely connected volunteer groups described in the previous chapter. The solutions focus primarily on information operations techniques instead of the traditional technology or law enforcement based approaches. The Summary briefly reviews the work and findings, as well as discusses future research.

The nature of the topic

Cyber security in general and the malicious volunteers in cyber conflict topic in particular are best addressed in a multi-disciplinary approach, using elements from informatics, military science (or art, depending on one's viewpoint), social science, system science, political science, information technology, media, psychology and law studies, to name a few. This is also reflected in the newly created international Cyber Security Master's program, taught jointly at Tallinn University of Technology and Tartu University. Next to "tech" oriented courses (focusing on things like malware analysis and monitoring solutions) it also contains a number of other courses like cyber security management, military history and cyber security law.

Obviously, I cannot claim in depth expertise in all these fields. I have made and effort, however, to draw upon concepts from the various sciences that overlap this area of inquiry in order to address this complex and multi-disciplinary problem.

Acknowledgements

Writing this thesis relied heavily on the support from my family and friends, who have believed in me and given me the motivation to complete it.

I wish to thank my co-advisor Professor Peeter Lorents for our countless intellectual bouts on the workings of science and for encouraging me on this road of discovery. I also wish to thank Professor Ahto Buldas for co-advising me and for providing a personal example as a scientist. Another key figure in my academic maturing process is Professor *Emeritus* Leo Võhandu, whose seminars have done much to broaden my scientific horizons over the years.

I wish to thank Prof Dorothy Denning (Naval Postgraduate School), Dr Jose Nazario (Arbor Networks), Prof Samuel Liles (Purdue University Calumet), Mr Jeffrey Carr (Greylogic) and Mr Kenneth Geers (CCD COE) for their useful comments to my cyber militia models.

This work could not have taken place without the support of the Estonian Defence Forces and the Cooperative Cyber Defence Centre of Excellence. In particular, I am grateful to Major (R) Raul Rikk and Colonel Ilmar Tamm for enabling my research and for providing me with challenging opportunities to grow.

Last, but not least, I would like to thank every colleague, teacher and (fellow) student who has provided me with new knowledge and insight.

1. Related work

This research does not fit well under any single heading in science. I have drawn inspiration from a number of very different disciplines and I hope that this thesis also proves interesting to scholars and practitioners in various fields. This section is not meant to provide full detail of every possible field of science that is connected to this work, but rather to highlight the areas that directly influence or are influenced by my work.

1.1 Military art and science

It may come as a surprise, but the military community has not come to agreement on whether the conduct of warfare is an art or a science. Probably the best known writing on the conduct of warfare is the "Art of War" by Sun-Tzu (see Sawyer 1994). The genius of that (short) book is that it primarily addresses warfare in the abstract and has therefore stayed relevant over thousands of years.[1] While the book offers a number of well known quotes, there are a few that are particularly important for this work:

- *"Warfare is the greatest affair of state, the basis of life and death, the Way to survival or extinction. It must be thoroughly pondered and analyzed."* While cyber attacks mostly do not amount to warfare, they can be considered as manifestation of (cyber) conflict. The Estonian case in 2007 shows that cyber conflict can be a matter of national security, even if the attacks are difficult to attribute to a state actor. This fact has provided the primary motivation for my research.
- *"Thus it is said that one who knows the enemy and knows himself will not be endangered in a hundred engagements."* This problem is particularly difficult to solve in cyber conflict. Known as the attribution problem, it stems from the fact that the standard mode of offensive operations in cyberspace is anonymous and that it is rarely possible to be certain about the source, extent and goal of a cyber attack. One of the goals of this work is to provide a better overview of a specific type of actors in cyber conflicts.
- *"Subjugating the enemy's army without fighting is the true pinnacle of excellence."* In Chapter 5 I have knowingly steered away from "standard" approaches, such as forensic investigation, law enforcement, etc. While they are of great value, they still have limitations. For example, it is often not possible to attribute a specific cyber attack, so it is not possible to take law enforcement action against the attacker. Therefore, I have tried to find

[1] Although the book contains references to the conditions and technologies of the time (such as chariots), it is still largely an abstract treatise on the nature of human conflict. Today, it is widely used in circles outside the military, particularly in the business world.

alternative ways of neutralizing the threat that do not necessarily require definite attribution. Overall, these approaches can be described as information operations.

- *"Warfare is the Way of deception."* This quote provides the inspiration of using information operations to deal with the threat from cyber militias.

To paraphrase another famous author in the military circles, Carl von Clausewitz, cyber conflict is the continuation of politics by other means (see von Clausewitz 1997). In the 21st century, those other means can easily be cyber attacks. This is also why I have chosen to limit my research to politically motivated cyber attack(er)s.

Moving closer to the cyber realm, Rattray (2001) has written an interesting book on "Strategic Warfare in Cyberspace". In it, he reviews the development of the US Air Force in the 20th century and draws analogies to the current developments in cyberspace. It is interesting to see the similarities of the discussions about air power that took place roughly one hundred years ago and the discussions of today about cyber power. The legal implications of a new fighting domain, the question about integrating the new force with the tried and true approaches, and even the questions of whether or not a new breed of warrior is needed follow the same pattern. The latter issue is also raised by Conti and Surdu (2009) who have posited the question of whether there is a need for a completely new arm of the (US) military that would deal with cyber conflict and cyber warfare. In their paper they also discuss the different requirements for the cyber warrior – what properties are important, how their training and career is different, etc.

Rios (2009) analyzes cyber warfare from the perspective of the US Marine Corps maneuver warfare doctrine and concludes that the cyber force is best used in support of, or as the main effort of the military campaign that includes conventional forces, as opposed to launching a purely cyber campaign. These thoughts are met by Bernier and Treurniet (2010) who also call for the integration of cyber and conventional operations.

Liles (2010) compares cyber conflict to low intensity conflict and insurgency. A similar approach is taken by Lemay, Fernandez and Knight (2010), who consider a low intensity cyber conflict where the adversary is bled dry by countless pinprick attacks. While each single attack is below the threshold where one is motivated to respond, the numbers add up and seriously weaken the target in the long run.

Some researchers have made efforts to link elements of military theory and doctrine to cyber conflict by addressing concepts like OODA[2] loop, DIMEFIL,[3]

---

[2] Colonel John Boyd of the US Air Force developed the OODA loop concept to address the combat operations cycle. It consists of a cycle of observation, orientation, decision and action (feedback loop). See Coram (2002) for more details.

PMESII[4] and Warden's five ring targeting model[5](see, for example, Arwood, Mills & Raines 2010; Veerasamy 2010). While this work is essential in bridging the gap between experts in military theory and the newly developing field of cyber conflict research, it is still far from complete.

1.2 The Law of Armed Conflict

There seems to be relative consensus in the world about cyber crime[6] and, in general, nations are taking steps to address it with national criminal law. There is even an international instrument – the Council of Europe (2001) Convention on Cyber Crime, which provides a legal framework for dealing with international cyber crime. While it is not ratified by many countries, it does offer a way forward. However, the picture is quite different in terms of politically motivated cyber attacks. Some authors argue that a treaty will not solve this problem, since some states are interested in exploiting the grey areas in cyberspace (see, for example, Geer 2010; Leaven & Dodge 2010), while others argue for more relaxed rules for attributing cyber attacks to states (see, for example, Goodman 2010; Shackelford 2010).

One way to look at this problem is to explore the Law of Armed Conflict (LOAC), which can be divided into two broad categories: *jus ad bellum* and *jus in bello*.[7] This body of law is generally applicable in case of armed conflict. However, therein lies the problem – it is unclear if and when cyber conflict can be considered armed conflict. For example, Watts (forthcoming) points out that low intensity cyber conflict will likely not trigger the LOAC mechanism.

One of the important milestones in LOAC as it applies to cyber conflict is a pair of articles by Schmitt (1999, 2002), which provide the so called "Schmitt analysis" for determining whether a cyber attack could be considered a "use of

---

[3] DIMEFIL stands for the instruments of national power: Diplomatic, Informational, Military, Economic, Financial systems, Intelligence and Law Enforcement

[4] PMESII stands for a targeting methodology that takes into account the Political, Military, Economic, Social, Informational and Infrastructure factors.

[5] Warden's five ring targeting model (see Warden 1995) addresses targeting at the strategic level and is visualised by concentric circles representing leadership (centre), system essentials, infrastructure, population and fielded military.

[6] In this context the cyber crime is limited to crime motivated by personal gain, such as money.

[7] *Jus ad bellum* refers to the "body of international law governing the resort to force as an instrument of national policy" or in other words the acts that can (legally) lead to war. (Schmitt 1999) *Jus in bello* refers to the "body of law concerned with what is permissible, or not, during hostilities, irrespective of the legality of the initial resort to force by the belligerents" or in other words – things occurring during wartime. (Schmitt 2002)

force"[8] and describe the legal aspects of using cyber attacks during armed conflict. Professor Schmitt is currently chairing a working group that is writing the Manual on International Law Applicable to Cyber Conflict, also known as the Tallinn Manual, that will bring much needed clarification into the issue upon its completion in 2012 (CCDCOE 2011).

1.3 Information operations

Much of the Information Operations (IO) doctrine is inspired by the United States approach. Joint Publication 3-13 (Joint 2006) is often cited in order to explain the typical core components of IO: Psychological Operations[9], Military Deception,[10] Operational security, Electronic Warfare, and Computer Network Operations (CNO). There are numerous works that delve deeper into the field of information warfare and information operations (see, for example, Armistead 2004, 2007; Denning 2004; Wilson 2007), although only recently has there been a strong focus on CNO. This thesis is primarily concerned with the application of psychological operations and military deception methods in order to achieve effects in cyber security (bearing in mind that the target audience is not a military force).

Mulvenon (1999) and Perry (2007) find that the Chinese IO doctrine is actually adopted from the corresponding US doctrine and has been modified with some Chinese concepts, such as "People's War" and "killing with a borrowed sword". These concepts are also considered by Wu (2004), in his analysis of information warfare research in China. People's War refers to the idea of *levée en masse*, where individuals will take up arms to fight the enemy, without any direct support from the state. Killing with a borrowed sword refers to the idea that one can use a third party's assets to strike the blow against the adversary, thus providing ambiguity and deniability.

---

[8] The Schmitt analysis looks at six different attributes of an event: severity, immediacy, directness, invasiveness, measurability and presumptive legitimacy. For an example of the use of the Schmitt analysis, see (Michael, Wingfield & Wijesekera 2003).

[9] Psychological operations are "planned operations to convey selected truthful information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately, the behavior of their governments, organizations, groups, and individuals." (Joint 2006)

[10] "MILDEC is described as being those actions executed to deliberately mislead adversary decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly forces' mission." (Joint 2006)

1.4 Cyber security and national security

During the late 1990's the issue of cyber security [11] started to gain importance in national security circles. There is little doubt that today it is a key (perhaps overhyped) component of the (inter)national security debate. For example, cyber threats are among the threats specifically listed in the NATO Strategic Concept (NATO 2010). Nissenbaum (2005), among others, has used the securitization (or Copenhagen school) theory (see Buzan, De Wilde & Waever 1997) to show how the concept of cyber security has been (artificially) raised into the national security debate. This idea is also developed by Hare (2010), who compares four different countries and their approach to cyber security in the framework of power and social cohesion. However, some scholars point out the problem that the policymakers do not know the issue well enough to make informed decisions (see, for example, Cornish, Livingstone, Clemente and Yorke 2010).

An important issue in cyber security is also the emergence of nation-states that possess various levels of offensive cyber capability. For example, Billo and Chang (2004) provide an analysis of the capabilities of China, India, Iran, North Korea, Pakistan and Russia to conduct cyber warfare. While this study is somewhat out of date, it provides a convenient backdrop to some of the more recent studies, such as (Fritz 2008, Perry 2007, Thomas 2008). Comparing these studies shows that there have been substantial developments in offensive cyber capability, especially in China (see, for example, Thomas 2004, 2005, 2007, 2008). Another issue is the proliferation of politically motivated misuse of cyberspace, such as the examples of censorship, hactivism, crime and espionage covered in (Deibert & Rohozinski 2010).

1.5 Cyber forces and volunteer cyber militia

There are many different ways for a person to participate in cyber conflict. The literature can be broadly divided into two groups. The first addresses various government forces and organizations while the second looks at the issues of non-state groups and individual (h)activism.

Not surprisingly, there are a number of works that address the developments in the US military over the past twenty years. These include the works by Starr, Kuehl and Pudas (2010), Wilson Wrona (2005) and Lynn (2010). An interesting issue is raised by Yurcik and Doss (2001) who claim that US military considered the use of cyber attack as early as the Kosovo campaign. Other

[11] The cyber security of today has evolved over time from concepts like data and information security, computer security, network security, information assurance, etc. That does not mean that all these phrases are synonyms. Rather, they look at various aspects of the cyber security issue.

countries, especially China and Russia, also receive analysis. For example, Krekel et al. (2009) do a very thorough analysis of China, as does Thomas (2008). Billo and Chang (2004) contribute a broader overview of several counties.

Another noticeable trend in the government approach is the issue of training and educating government cyber forces. For example, Huhtinen, Armistead and Schou (2010) look at this from the broader IO context, whereas Scweitzer and Fulton (2010) and Starr, Kuehl and Pudas (2010) focus more on the cyber specific context. They all agree that the cyber warrior requires a somewhat different approach in selection and training compared to traditional services.

The question of non-state groups and hactivism is of special interest for this work. It should be identified from the start that there are varying degrees of digital violence and political zeal in the groups. Williams and Arreymbi (2007) describe how the information technology allows people to form virtual "cyber tribes" regardless of their location, as long as they find a common interest. This explains the proliferation of politically motivated hacking and hackers in general, as described by Meikle (2009), Samuel (2004), Denning (1999, 2010), Alleyne (2010), Karatzogianni (2010) and Chiesa, Ducci and Ciappi (2009). An interesting point is raised in (Hintz & Milan 2010) – technology enthusiast groups (including hackers) are notoriously vary of researchers and are therefore very difficult to study.

Samuel (2004) investigates the various types of politically motivated hactivism and brings out two ways of looking at it. One way is to look at hactivism as a form of civil disobedience, where cyber attacks are seen as a non-violent way of protest. This view is partially supported by Meikle (2009), who explores the differences between hactivism, terrorism and electronic civil disobedience. The other way, which is also the approach of this work, is to look at hactivism as a cyber security problem. For example, Denning (1999) makes a distinction between online activism and hactivism, where the latter is seen as criminal activity. On the other hand, The Hacker Profiling Project (Chiesa, Ducci & Ciappi 2009) points out that hacking is in its heart an apolitical phenomenon, so politically motivated hacking is a tainted activity in the eyes of "real hackers". For the cyber security community, Denning's view is clearly easier to accept and many scholars have described and analyzed various cases of politically motivated cyber attacks from this perspective (see, for example, Allen & Demchak 2003; Carr 2009; Denning 2010; Nazario 2009; Wilson Wrona 2005).

West and Latham (2010) look at the power of Web 2.0 solutions to recruit volunteers into (virtual)(terrorist) organizations and to manage said organizations. They point out that it is possible to create an anonymous and free social network with existing tools, so the groups do not have to congregate at well known venues if they prefer to keep a lower profile. This aspect is quite important in this work, especially in the context of (**II**) and (**III**). The topic of extremist use of the Internet is also well covered by Bardin (2010).

2. The systematic approach

The method, structure and backdrop of this work are provided by the systematic approach developed by Lorents (see, for example, Lorents 2001a, 2008; **V**), which includes the *systematic approach principle: anything that can be reasonably represented as a system, should be*. This Chapter is based on Lorents' contribution in (**I**) as well as on (Lorents 2006).

Note that there are other definitions to the concepts identified in this chapter and some of these are subject to hot debate in the scientific community. *The aim in presenting this approach here is not to settle these arguments, but to provide the key to understanding the contributions described in later chapters.*

2.1 Why systematic approach?

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 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. As described in Chapter 3, the problem with situation descriptions is often the fact that there can be multiple meanings for a particular term, or multiple terms for a particular meaning. For example, 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 order to effectively handle events in cyberspace, we (humans) first need to be able to clearly describe these concepts, situations and events, and any constraints that apply to them. Fortunately, one of my advisors, professor Lorents, had spent a number of years developing a well founded framework (described below) that is rooted in formal mathematical theories (algebraic systems theory, model theory, proof theory, etc.) and can be extended for use in cyber security research.

In this Chapter we focus on understanding terms that are related to systems (including the life and death of systems), information, operating with information and the problems associated with securing information, including confidentiality, availability and integrity. *These terms play an important role later in the thesis, in discussions about cyber weapons, cyber conflict, as well as reasoning about describing, controlling and neutralizing cyber militias.*

2.2 Knowledge, Data and Information

In order to explain the concept of information we use the definitions of knowledge and data (see, for example, Lorents 2001a, 2008; **V**). 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 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*. This means that there could be many denotation 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*. This refers to the property that allows to "carry over" relationships, or in short (A∫B)&(B∫C)→(A∫C).
- *equality*. 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)).

Definition 1. If some objects A and B have the relationship (A∫B), then the ordered pair ⟨A,B⟩ is called **knowledge** (Lorents 2001a, 2006, 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 Vatican are European countries.

Definition 3. **Information** is either knowledge or data.

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.

2.3 Systems and the systematic approach

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.

Definition 4. A **system** is a structured set of elements. 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 5. The approach where the observed things are considered as systems, or belonging to systems, is called the **systematic approach**.

Definition 6. The process that uses certain influence factors to move a system from one state to another (desired) state, is called **system control**.

Definition 7. Let there be two systems A and B, which may in special cases be the same system. If all possible states of system A can be reached or avoided by using appropriate influence factors on system B, then system A **completely controllable** by system B. If, on the other hand, none of the possible states of system A can be reached or avoided by using any influence factors on system B, then system A is **completely uncontrollable** by system B. A system is **partially controllable** or **partially uncontrollable**, if it is neither completely controllable nor completely uncontrollable.

Definition 8. The influence factors required for system control are called **control measures**. A system of control measures is called a **control system** or a **control mechanism**.

Definition 9. A system is **absolutely dead in terms of elements**, if all elements of the system's main set have ceased to exist.

Definition 10. A system is **absolutely dead in terms of relations**, if all properties and relations in the system's signature have ceased to exist.

Definition 11. If at least one element disappears from the main set of the system during the system's transition from one state to the next, then we say that the system is **more dead (less alive) in terms of elements** in the second state.

In terms of cyber militia, this would mean that if a member (element) of the militia is removed from the system (for example, he is arrested or he is convinced to leave), the militia would be **damaged in terms of elements.**

Definition 12. If at least one element disappears from the signature of the system during the system's transition from one state to the next, then we say that the system is **more dead (less alive) in terms of relations** in the second state.

In terms of cyber militia, if an element from the signature of the system, such as the relation "trust", is broken between some or all the elements of the system, then the system would be **damaged in terms of relations**.

Definition 13. The parts of the system that cause the system's death if they are removed are called the **vital components** of the system.

Definition 14. 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 (operating) 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.

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 (**IV;V**). 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. 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 the modern society. Communication and control, however, characterize the research field of cybernetics, which is the origin of the term "cyber" (Wiener 1948).

2.4 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.

2.4.1 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 to computer 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 maximum information transfer rate: $K \leq W \cdot log_2(1+P/N)$. (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.

2.4.2 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. 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.

2.4.3 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 16. The information X, A or B (where $X=\langle A,B\rangle$ and $A \int B$) is **confidential** from system S if the 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.

2.5 Application of the systematic approach

Chapters 4 and 5 present the cyber militia models from the viewpoint of systems. Specifically, they are considered as systems where the elements, as well as their properties and relations are identified in text as *E[member], P[description]* and *R[description]*, respectively (they are often identified in parentheses after the phrase, sentence or paragraph that describes or identifies them). In some cases, the property is optional (can exist or not exist, depending on the circumstances). For example, P[state ties] in the Hierarchy model is optional, since hierarchies are not necessarily state sponsored. However, it is still included as a property, as both cases (there are state ties or there are no state ties) are of interest.

For the sake of convenience, multiple properties that are relevant in a specific case are displayed in the same bracket (for example, P[A, B, C]), whereas in some cases the relationship is described in a loose format (for example, R[trust between all members] represents an all-to-all trust relationship between the members of the militia) and for all cases the individuals are not shown in the notation. In some cases the item of interest is a metalevel property or relation of the system of cyber militia. This is represented as *Pm[description]* or *Rm[description]*. In other cases, an action (vs. property or relation) implies something. For example, (attacking Forum) → P[motivation]. It is sometimes necessary to indicate the role of the friendly agent in the relationship. In such a case the corresponding role is shown in italics (for example, R[*provider*, receiver]). In addition, three types of logic operators are used in the text: negation (¬), conjunction (&) and implication (→).

3. Key concepts in cyber conflict

The issue of identifying key concepts in cyber conflict comes from the need to explain the national security aspects of cyber security (especially if the security situation assumes adversarial conditions). In such discussions, concepts like cyber attack, cyber weapon and cyber warfare are used very liberally and rarely do the parties know what the other party actually means. To make matters worse, people from different areas of expertise (for example, lawyers, military officers, politicians, computer security experts, etc.) are usually needed to address these national security problems.

This Chapter describes my contribution to defining the key concepts in cyber conflict by extending the knowledge based definition framework described in Chapter 2. The primary contribution of this Chapter is developed in (**I, IV, V**), in collaboration with Lorents (*where my contribution to the work presented in this chapter is 50% or more*). Note, however, that there are other definitions to these concepts. *The purpose of this work is to provide a well founded and relatively easy to understand system of definitions, not to replace existing definitions altogether*.

3.1 Information technology 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 1. 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 2. 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 3. 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 to 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 always true. The targets of cyber weapons are located in cyberspace, which reinforces the connection with the "cyber" prefix.

3.2 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 4. **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 5. 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 6. Cyber espionage is the use of cyber attacks to cause a loss of confidentiality of the target system.

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

Definition 7. 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 8. Cyber war is a cyber conflict between state actors.

While cyber conflicts can take place between state actors, non-state groups and individuals, a war should be limited to state actors.[12] For example, military

[12] Without this limitation, war qould be ubiquitous and constant, devaluing the term into uselessness.

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 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.

3.3 Cyberspace and cyber society

Definition 9. **Cyberspace**[13] is a time-dependent set of interconnected information systems and the human users that interact with these systems.

As can be seen from this definition, we approach cyberspace from a wider perspective than most researchers – namely we include the human users. The reason for this is that we believe that cyberspace is chiefly relevant at the human-computer interface, whether that interface is the input-output system of a computer, or a controller that effects some physical change in the environment of the user (for example, turning off the lights in the building).

Definition 10. A **cyber society** is a society where computerized information transfer and information processing is (near) ubiquitous and where the normal functioning of this society is severely degraded or altogether impossible if the computerized systems no longer function correctly.

The definition of cyber society explains my motivation for studying this problem from the threat perspective. As cyber weapons become more sophisticated and at the same time more available for the general public (and offensively oriented cyber militias), the security risks of the cyber society increase. Therefore, it is prudent to analyze the various threats and develop countermeasures and defenses against them.

[13] This term was originally introduced in 1984 in science fiction literature (Gibson 2000), but has now made it into everyday use and is especially relevant in the context of this work.

4. Offensive volunteer cyber militia

Information technology has become ubiquitous. Computers are no longer tools reserved for the military, scientific and intelligence community. Computing devices are cheap, easy to use, easily available and built with multi-purpose functionality. While this is a very beneficial set of attributes, it also introduces new threats. One of these threats is the fact that people with low resources and skills can use these devices to perform cyber attacks.

Cases like the 2007 cyber attacks against Estonia are a good example where an informal non-state cyber militia has become a threat to national security. In order to better understand the threat posed by these volunteer cyber militias I provide three models of how such groups can be organized and analyze the strengths and weaknesses of each using the concepts presented in Chapters 2 and 3.

The three models considered are the Forum, the Cell and the Hierarchy. The models are applicable to groups of non-trivial size, which require internal assignment of responsibilities and authority. This chapter is based on (**II**; **III**) and builds on the concept of volunteers as described in (**VI**, Ottis 2009).

4.1 Method and limitations

In this Chapter I use theoretical qualitative analysis and the systematic approach (see Chapter 2) in order to describe the attributes, strengths and weaknesses of three offensively oriented cyber militia models. Note that the description of the models is based on theoretical reasoning and expert opinion. It offers abstract theoretical models in an ideal setting, and therefore some elements in a real cyber militia may not meet the property and relation requirements. For example, while the Forum model assumes that members are anonymous, some people may actually identify themselves during actual cyber conflicts. Therefore, there may not be a full match to any model in reality or in the examples provided. It is more likely to see either combinations of different models or models that do not match the description in full. On the other hand, the models should serve as useful frameworks for analyzing volunteer groups in the current and coming cyber conflicts.

I have chosen the three plausible models based on what can be observed in recent cyber conflicts. The term model refers to an abstract description of properties and relationships between members of the cyber militia, including command, control and mentoring relationships, as well as the operating principles of the militia.

4.2 The Forum

The global spread of the Internet allows people to connect easily and form „cyber tribes“, which can range from benign hobby groups to antagonistic ad-hoc cyber militias. (Williams and Arreymbi 2007, Ottis 2008, Carr 2009,

Nazario 2009, Denning 2010) In the case of an ad-hoc cyber militia, the Forum unites like-minded people who are willing and able to use cyber attacks in order to achieve a political goal. It serves as a command and control platform where more active members can post motivational materials, attack instructions, attack tools, etc. (Denning 2010)

This particular model, as well as the strengths and weaknesses covered in this section, are covered in more detail in the next Chapter, which also introduces some countermeasures against it. A good example of this model in recent cyber conflicts is the stopgeorgia.ru forum during the Russia-Georgia war in 2008 (Carr 2009).

4.2.1 Attributes

The Forum is an on-line meeting place for people who are interested in a particular subject. I use Forum as a conceptual term referring to the people who interact in the on-line meeting place. The technical implementation of the meeting place could take many different forms: web forum, Internet Relay Chat channel, social network subgroup, etc. It is important that the Forum is accessible over Internet and preferably easy to find. The latter condition is useful for recruiting new members and providing visibility to the agenda of the group.

The Forum mobilizes in response to an event that is important to the members (P[motivation]). While there can be a core group of people who remain actively involved over extended periods of time, the membership can be expected to surge in size when the underlying issue becomes "hot" (P[ad hoc participation]). Basically, the Forum is like a flash mob that performs cyber attacks instead of actions on the streets. As such, the Forum is more ad-hoc than permanent, because it is likely to disband once the underlying event is settled.

The membership of the Forum forms a loose network centered on the communications platform, where few, if any, people know each other in real life and the entire membership is not known to any single person. Most participate anonymously, either providing an alias or by remaining passive on the communication platform (P[anonymous, not vetted]). In general, the Forum is an informal group, although specific roles can be assumed by individual members (P[role]). For example, there could be trainers, malware providers, campaign planners, etc. This also implies a (one-to-one, one-to-many, many-to-one, or many-to-many) relationship between, for example, trainer and trainee (R[provider, receiver]).[14] Some of the Forum members may also be active in

[14] The provider-receiver relationship is an attempt to generalize the various role based relationships, since there is no defined and finite list of possible roles. It should be noted that a single member can have multiple relationships and can be on either side of

cyber crime (P[criminal history]). In that case, they can contribute resources such as malware or use of a botnet to the Forum.

The membership is diverse, in terms of skills (P[skill]), resources (P[resources]) and location (P[location]). While there seems to be evidence that a lot of the individuals engaged in such activities are relatively unskilled in cyber attack techniques (Carr 2009), when supplemented with a few more experienced members the group can be much more effective and dangerous (Ottis 2010).

Since most of the membership remains anonymous and often passive on the communications platform, the leadership roles will be assumed by those who are active in communicating their intent, plans and expertise. (Denning 2010) However, this still does not allow for strong command and control, as each member can decide what, if any, action to take (P[no command authority]).

As a result, we get a signature of **P[motivation, ad-hoc participation, anonymous, not vetted, role, criminal history, skill, resources, location, no command authority]** and **R[provider, receiver]**, where **P[motivation, anonymous]** and **R[provider, receiver]** are vital components. Based on this signature and the idea of damaging systems (in terms of elements or relations), we can now analyze the strengths and weaknesses of the Forum.

4.2.2 Strengths

One of the most important strengths of the Forum is that it can form very quickly. Following an escalation in the underlying issue, all it takes is a rallying cry on the Internet and within hours or even minutes the volunteers can gather around a communications platform, share attack instructions, pick targets and start performing cyber attacks. P[motivation, ad-hoc participation, not vetted] → Pm[quick to form] The Forum is also easily scalable, as anyone can join and there is no lengthy vetting procedure P[not vetted, anonymous] → Pm[scalable].

The diversity of the membership means that it is very difficult for the defenders to analyze and counter the attacks. The source addresses are likely distributed globally (black listing will be inefficient) and the different skills and resources ensure heterogeneous attack traffic (no easy patterns). Experienced attackers can use this to conceal precision strikes against critical services and systems. P[anonymous, skill, resources, location] → Pm[difficult to pattern match]

While it may seem that neutralizing the communications platform (via law enforcement action, cyber attack or otherwise) is an easy way to neutralize the militia, this may not be the case. The militia can easily regroup at a different communications platform in a different jurisdiction. Attacking the Forum

---

the relationship. For example, a person could be a trainer (provider) but use the attack kits uploaded by someone else (receiver).

directly may actually increase the motivation of the members. (attacking Forum) → P[motivation]

Last, but not least, it is very difficult to attribute these attacks to a state, as they can (seem to) be a true (global) grass roots campaign, even if there is some form of state sponsorship. P[anonymous, no command authority, location, resources] → Pm[state deniability]

4.2.3 Weaknesses

A clear weakness of this model is the difficulty to command and control the Forum. Membership is not formalized and often it is even not visible on the communication platform, because passive readers can just take ideas from there and execute the attacks on their own. This uncoordinated approach can seriously hamper the effectiveness of the group as a whole. It may also lead to uncontrolled expansion of conflict, when members unilaterally attack third parties on behalf of the Forum. P[no command authority, anonymous, no vetting] → Pm[weak command and control]

A problem with the Forum is that it is often populated with people who do not have experience with cyber attacks. Therefore, their options are limited to primitive manual attacks or preconfigured automated attacks using attack kits or malware. (Ottis 2010) They are highly reliant on instructions and tools from more experienced members of the Forum. P[skill, resources, role] & R[provider, receiver] → Pm[unsophisticated attack capability]

The Forum is also prone to infiltration, as it must rely on relatively easily accessible communication channels. If the communication point is hidden, the group will have difficulties in recruiting new members. The assumption is, therefore, that the communication point can be easily found by both potential recruits, as well as infiltrators. Since there is no easy way to vet the incoming members, infiltration should be relatively simple. P[anonymous, not vetted] → Pm[easy to infiltrate]

Another potential weakness of the Forum model is the presumption of anonymity. If the membership can be infiltrated and convinced that their anonymity is not guaranteed, they will be less likely to participate in the cyber militia. (perception of anonymity removed) → ¬P[motivation]

4.3 The Cell

Another model for a volunteer cyber force that has been seen is a hacker cell. In this case, the generic term hacker is used to encompass all manner of people who perform cyber attacks on their own, regardless of their background, motivation and skill level. It includes the hackers, crackers and script kiddies described by Young and Aitel (2004), as well as the more detailed list described by Chiesa, Ducci and Ciappi (2009). The hacker cell includes several hackers who commit cyber attacks on a regular basis over extended periods of time.

Examples of hacker cells are Team Evil and Team Hell, as described in Carr (2009).

4.3.1 Attributes

Unlike the Forum, the Cell members are likely to know each other in real life, while remaining anonymous to the outside observer (P[anonymous to outsiders; identified inside cell]). Since their activities are almost certainly illegal, they need to trust each other (R[trust between all members]). This limits the size of the group and requires a (lengthy) vetting procedure for any new recruits (P[vetted]). The vetting procedure can include proof of illegal cyber attacks (P[criminal history]).

The command and control structure of the Cell can vary from a clear self-determined hierarchy to a flat organization, where members coordinate their actions, but do not give or receive orders. In theory, several Cells can coordinate their actions in a joint campaign, forming a confederation of hacker cells.

The Cells can exist for a long period of time, in response to a long-term problem, such as the Israel-Palestine conflict. The activity of such a Cell ebbs and flows in accordance with the intensity of the underlying conflict. The Cell may even disband for a period of time, only to reform once the situation intensifies again. (P[long term participation])

Since hacking is a hobby (potentially a profession) for the members, they are experienced with the use of cyber attacks (P[skilled, confident]). One of the more visible types of attacks that can be expected from a Cell is the website defacement. Defacement refers to the illegal modification of website content, which often includes a message from the attacker, as well as the attacker's affiliation. The Zone-H web archive lists thousands of examples of such activity, as reported by the attackers. Many of the attacks are clearly politically motivated and identify the Cell that is responsible.

Some members of the Cell may be involved with cyber crime.[15] For example, the development, dissemination, maintenance and use of botnets for criminal purposes. These resources can be used for politically motivated cyber attacks on behalf of the Cell. (P[criminal history, resources])

This gives us the signature **P[anonymous to outsiders, known inside cell, vetted, criminal history, long term participation, skilled, confident, resources]** and **R[trust between all members]**, where **R[trust between all members]** is a vital component.

[15] This does not mean that politically motivated cyber attacks are not cyber crime. Instead, the distinction is made regarding "traditional" cyber crime that is primarily motivated by personal gain.

4.3.2 Strengths

A benefit of the Cell model is that it can mobilize very quickly, as the actors presumably already have each other's contact information. In principle, the Cell can mobilize within minutes, although it likely takes hours or days to complete the process. P[identified inside cell, vetted, long term participation] → Pm[quick to form]

A Cell is quite resistant to infiltration, because the members can be expected to establish their hacker credentials before being allowed to join. This process may include proof of illegal attacks. P[vetted, criminal history] → Pm[resistant to infiltration]

Since the membership can be expected to be experienced in cyber attack techniques, the Cell can be quite effective against unhardened targets. However, hardened targets may or may not be within the reach of the Cell, depending on their specialty and experience. Prior hacking experience also allows them to cover their tracks better, should they wish to do so. P[skilled, long term participation, criminal history, anonymous to outsiders] → Pm[effective, difficult to trace]

4.3.3 Weaknesses

While a Cell model is more resistant to countermeasures than the Forum model, it does offer potential weaknesses to exploit. The first opportunity for exploitation is the hacker's ego. P[confident] → Pm[exploitable] Many of the more visible attacks, including defacements, leave behind the alias or affiliation of the attacker, in order to claim the bragging rights. (Carr 2009) This seems to indicate that they are quite confident in their skills and proud of their achievements. As such, they are potentially vulnerable to personal attacks, such as taunting or ridiculing in public. Stripping the anonymity of the Cell may also work, as at least some members could lose their job and face law enforcement action in their jurisdiction ¬P[anonymous to outsiders] → ¬E[member]. (Carr 2009) As described in (**III**), it is probably not necessary to actually identify all the members of the Cell. Even if the identity of a few of them is revealed or if the corresponding perception can be created among the membership, the trust relationship will be broken and the effectiveness of the group will decrease. ¬P[anonymous to outsiders] → ¬R[trust between all members]

Prior hacking experience also provides a potential weakness. It is more likely that the law enforcement know the identity of a hacker, especially if he or she continues to use the same affiliation or hacker alias. P[skilled, criminal history] → P[known to law enforcement] While there may not be enough evidence or damage or legal base for law enforcement action in response to their criminal attacks, the politically motivated attacks may provide a different set of rules for the local law enforcement.

The last problem with the Cell model is scalability. There are only so many skilled hackers who are willing to participate in a politically motivated cyber

attack (Chiesa, Ducci & Ciappi 2009). While this number may still overwhelm a small target, it is unlikely to have a strong effect on a large state. P[vetted, skilled] & R[trust between all members] → Pm[not scalable]

4.4 The Hierarchy

The third option for organizing a volunteer force is to adopt a traditional hierarchical structure. This approach is more suitable for government sponsored groups or other cohesive groups that can agree to a clear chain of command. For example, the People's Liberation Army of China is known to include militia type units in their information warfare battalions. (Krekel et al. 2009)

4.4.1 Attributes

The Hierarchy model is similar in concept to military units, where a unit commander exercises power over a limited number of sub-units or people (P[formal role, key person],R[commander, subordinate]). The number of command levels depends on the overall size of the organization.

Each sub-unit can specialize on some specific task or role. (P[formal role]) For example, the list of sub-unit roles can include reconnaissance, infiltration/breaching, exploitation, malware/exploit development and training. This specialization and role assignment allows the militia unit to conduct a complete offensive cyber operation from start to finish. Another aspect of a hierarchy is the potential for advancement according to role or attained skill level. (P[specialized, formal role, skill])

A Hierarchy model is the most likely option for a state sponsored entity, since it offers a more formalized and understandable structure, as well as relatively strong command and control ability. The control ability is important, as the actions of a state sponsored militia are by definition attributable to the state. (P[formal role, state ties], R[commander, subordinate])

However, a Hierarchy model is not an automatic indication of state sponsorship. Any group that is cohesive enough to determine a command structure amongst them can adopt a hierarchical structure. In fact, Williams and Arreymbi (2007) suggest that gaming communities can be a good recruiting ground for a cyber militia. Either way, a form of vetting is required before a position of authority is assigned. (P[vetted])

While the state sponsored militia can be expected to have identified membership (still, it may be anonymous to the outside observer) due to control reasons, a non-state militia can consist of anonymous members that are only identified by their screen names.

This gives us the signature **P[formal role, key person, specialized, skill, vetted, state ties]** and **R[commander, subordinate]**, where **P[key person]** and **R[commander, subordinate]** are vital components.

4.4.2 Strengths

The obvious strength of a hierarchical militia is the potential for efficient command and control. The command team can divide the operational responsibilities to specialized sub-units and make sure that their actions are coordinated. P[key person, formal role] & R[commander, subordinate] → Pm[efficient command and control]

A hierarchical militia may exist for a long time even without ongoing conflict. During "peacetime", the militia's capabilities can be improved with recruitment and training. This degree of formalized preparation with no immediate action in sight is something that can set the hierarchy apart from the Forum and the Cell. P[formal role] → Pm["peacetime" mission]

If the militia is state sponsored, then it can enjoy state funding, infrastructure, as well as cooperation from other state entities, such as law enforcement or intelligence community. P[state ties] → Rm[cooperation with state entities]

4.4.3 Weaknesses

A potential issue with the Hierarchy model is scalability. Since this approach requires some sort of vetting or background checks before admitting a new member, it may be time consuming and therefore slow down the growth of the organization. P[vetted] & R[commander, subordinate] → Pm[not easily scalable]

Another potential issue with the Hierarchy model is that by design there are key persons in the hierarchy. Those persons can be targeted by various means to ensure that they will not be effective or available during a designated period, thus diminishing the overall effectiveness of the militia. A hierarchical militia may also have issues with leadership if several people contend for prestigious positions. This potential rift in the cohesion of the unit can potentially be exploited by infiltrator agents. P[key person, vetted, role] & R[commander, subordinate] → Pm[single point of failure]

Any activities attributed to the state sponsored militia can further be attributed to the state. This means that a state sponsored offensive cyber militia is primarily useful as a defensive (or deterrent) capability between conflicts. Only during conflict can it be used in its offensive role. P[state ties] → Pm[attributable to state]

While a state sponsored cyber militia may be more difficult (but not impossible) to infiltrate, they are vulnerable to public information campaigns, which may lead to low public and political support, decreased funding and even official disbanding of the militia. P[state ties] → Pm[subject to public scrutiny and pressure] On the other hand, if the militia is not state sponsored, then it is prone to infiltration and internal information operations similar to the one considered at the Forum model. ¬P[state ties] → Pm[can be infiltrated]

Of the three models, the hierarchy probably takes the longest to establish, as the chain of command and role assignments get settled. P[formal role, skill, vetted, key person] → Pm[slow to establish] During this process, which could take days, months or even years, the militia is relatively inefficient and likely not able to perform any complex operations.

4.5 Comparison

When analyzing the three models, it quickly becomes apparent that there are some aspects that are similar to all of them. First, they are not constrained by location. While the Forum and the Cell are by default dispersed, even a state sponsored hierarchical militia can operate from different locations.

Second, since they are organizations consisting of humans, then one of the more potent ways to neutralize cyber militias is through information operations, such as persuading them that their identities have become known to the law enforcement, etc.

Third, all three models benefit from a certain level of anonymity. However, this also makes them susceptible for infiltration, as it is difficult to verify the credentials and intent of a new member.

On the other hand, there are differences as well. Only one model lends itself well to state sponsored entities (hierarchy), although, in principle, it is possible to use all three approaches to bolster the state's cyber power.

The requirement for formalized chain of command and division of responsibilities means that the initial mobilization of the Hierarchy can be expected to take much longer than the more ad-hoc Forum or Cell. In case of short conflicts, this puts the Hierarchy model at a disadvantage.

Then again, the Hierarchy model is more likely to adopt a "peace time" mission of training and recruitment in addition to the "conflict" mission, while the other two options are more likely to be mobilized only in time of conflict. This can offset the slow initial formation limitation of the Hierarchy, if the Hierarchy is established well before the conflict.

While the Forum can rely on their numbers and use relatively primitive attacks, the Cell is capable of more sophisticated attacks due to their experience. The cyber attack capabilities of the Hierarchy, however, can range from trivial to complex.

It is important to note that the three options covered here can be combined in many ways, depending on the underlying circumstances and the personalities involved.

5. Defending against volunteers

This chapter is based on (**III**) and addresses the Forum type of volunteer cyber militias discussed in Chapter 4. In addition to identifying the key properties and relations between the members of the militia, this chapter explores the options for neutralizing the cyber militia. Note, however, that while this chapter and my research narrows down the focus on the Forum type of militias, the same approach can be used on other militia models, and indeed, on other types of (cyber) forces in general.

5.1 On-line cyber militia

Let us define **cyber militia** as a group of volunteers who are willing and able to use cyber attacks in order to achieve a political goal. Let us further define **on-line cyber militia** as a cyber militia where the members communicate primarily via Internet and, as a rule, hide their identity (for example, by using a hacker alias). Cyber militias can be ad-hoc (gathering only for a specific occasion) or permanent. (P[volunteer, motivated, skill, resources, anonymous, ad-hoc participation, not vetted])

The word "volunteers" in the definition refers to people who participate in the cyber militia of their own free will. They do not get paid for their activities, nor do they have a contractual obligation to the militia. They have the right to choose their level of commitment and to leave the militia, if and when they wish. Therefore, volunteer soldiers who join a government run cyber attack unit are not considered a cyber militia.

The word "political" in the definition refers to all aims that transcend the personal interest of the volunteer. This includes religious views, nationalistic views, opinions on world social order etc.

In the context of this analysis, I am focusing on a subset of on-line cyber militias that meet the following criteria:

- The communication within the militia is centralized (R[sender, receiver])
- There is no direct state support or control of the militia (P[no state control])
- The members are loosely connected in real life (P[anonymous])

The centralized communication constraint is a fairly standard arrangement for communicating, preparing, planning and coordinating a cyber attack campaign of the cyber militia. Perhaps the most used communication channels are on-line forums and instant messaging services. (Carr 2009, Denning 2010) This is also very useful for the defending side, especially for observing, infiltrating and neutralizing the cyber militia.

Although the leadership or core group in a militia probably is personally acquainted, as a whole the members of the on-line cyber militia are loosely connected in real life. In this case loosely connected means that most members know no or few other members and nobody knows the entire membership in

person. This requires them to communicate over the Internet and coincidentally makes them more susceptible to infiltration and manipulation. While this constraint is not true in every case, it should be a safe assumption in large (numbering in the hundreds) militias and can also hold in smaller organizations.

From the forum posts it should be possible to identify the roles of the people in the cyber militia. Key "officer" roles include leaders, trainers, suppliers, while the rest could be categorized as soldiers, and "camp followers". Identifying the different roles in the organization offers individual targeting opportunities as well as potential avenues for infiltration. (P[role, key person], R[provider, receiver])

This gives us the signature of **P[volunteer, motivated, skill, resources, anonymous, not vetted, role, key person, no state control]** and **R[provider, receiver]**, where **P[motivated]** and **R[provider, receiver]** are **vital components** of the system. As such, these vital components should be the primary targets, as they have the greatest effect on the system (death). However, other elements may also be targeted in order to damage the system.

5.2 Neutralizing an on-line cyber militia

Using traditional law enforcement methods or military force is often not an effective approach, because personal attribution is seldom achieved and the militia members can reside in a number of different unfriendly and uncooperative jurisdictions. Therefore I will consider alternative tactics of neutralizing an on-line cyber militia. In particular, I will propose options from the strategic starting point of information operations and proactive defense.

An important caveat here is that I do not presume universal legality of any of the tactics. It would be very difficult to do, given that the legal status of the cyber militia and its actions may vary greatly, depending on the case. For example, the cyber militia may act completely within the legal framework of the host state. On the other hand, militia members could be considered illegal combatants who may be targeted for military action (Schmitt 2002). Therefore, the tactics below should be considered as theoretical options only, not as a policy manual for dealing with a cyber militia.

There are two points where the activity of an on-line cyber militia is potentially visible for observation. First, there are the logs at the targeted sites. Second, the shared communication channel (a forum, for example) where they gather, exchange opinions and plan their activities. The two places where the militia is visible are also the places where one can fight them.

Sun-Tzu said: ”Thus the highest realization of warfare is to attack the enemy’s plans; next is to attack their alliances; next to attack their army; and the lowest is to attack their fortified cities" (cited in Sawyer 1994). I will use this as a loose framework for considering tactics. The analogies do not need to be an exact fit and should be interpreted liberally.

5.2.1 Attacking plans

One way to neutralize the militia can be called poisoning the well tactic. It refers to corrupting the shared communication channel with de-motivational posts, self-destructive or ineffective attack tools and methods, bad targeting data, etc. As a result, the channel loses its effectiveness as a means for coordinating the actions of the militia, the members grow frustrated with apparent lack of coherence, and the aggression gets released inside the militia in the form of angry debate. If the militia is perceived as ineffective by the members, it will eventually disband (the system will die, as the members will no longer be a part of it). (P[anonymous, not vetted] & R[*provider*, receiver]) → (¬P[motivated])

An alternative approach would be to hijack the militia by shifting the debate to attacking other targets. This would basically deflect the blow from the original target, making it safe for the moment. (P[anonymous, not vetted] & R[*provider*, receiver]) → (¬P[motivated])

Yet another approach is to carry out an attack in the name of the militia against a powerful third entity in order to provoke a counterstrike against the entire militia (a false flag attack). In other words, pull a strong opponent into the fight, forcing the militia into defensive positions. As a result, the militia will have to drop its plans for the original target. (P[anonymous, not vetted] & R[*provider*, receiver]) → (¬P[motivated])

5.2.2 Attacking alliances

Presumably, members of the militia want to remain anonymous and would leave or become inactive if there was a serious chance of being personally identified. (¬P[anonymous, motivated]) This presents another opportunity to disband the militia from within by breaking the virtual alliances between militia members.

Without attribution there can be no personal consequences. On the other hand, if the anonymity is lost (or perceived lost by the membership), the forum will lose its trustworthiness. As a result, the militia will either disband or search for an alternative (clean) communication channel. However, since the infiltrated agents will also move over to the new channel, it would only be a temporary solution.

The question is, then, how to identify the members of the forum. In reality, it is probably not necessary to identify all or even most of the members. Most likely it is enough to break the cover of one or a few people, in order to create mistrust and fear of real life consequences in a considerable portion of the membership.

There are many ways to potentially achieve attribution of a few individuals. The simplest is to "break the cover" on infiltrated agents (can use fake identities, as they would be difficult to verify by other members) and have them "confirm" it. (P[anonymous, not vetted] & R[*provider*, receiver]) Another is to offer attack

tools to the forum that provide the information that is necessary for personal attribution (basically a Trojan). (P[anonymous, not vetted, role, resources] & R[*provider*, receiver]) Yet another is to correlate target log data with forum posts, and go through the legal channels. Of course, attribution may be achieved by simply arranging a meeting in real life. (P[anonymous, not vetted] & R[*provider*, receiver]) → ¬P[anonymous] → ¬P[motivated]

Note that it may not be necessary to actually follow up the attribution with legal or military action. Just posting the personal details of some users on the forum could be enough to make a considerable portion of the members leave. ¬P[anonymous] → ¬P[motivated]

5.2.3 Attacking the army

The loose analogy to an army in this case could be the cyber attacks organized by the militia (the soldiers that have marched to the city gates). Obviously, the defensive actions at the target come from the long list of standard cyber security measures. However, these can be deployed much more effectively, if the infiltrated agent can relay the attack plans to the defenders. Knowing when, where and how the attack will come makes the work of defenders much easier and blunts the effectiveness of the attackers. This, in turn, may have a demoralizing effect on the militia. (P[anonymous, not vetted] & R[*provider*, receiver]) → (¬P[motivated])

5.2.4 Attacking fortified cities.

Let us consider attacking the forum as the fortified city that serves as a home base for the cyber militia. Conceptually the easiest would be to use law enforcement to have it taken down, or if that fails, launch a denial of service attack against the server that hosts the service. Alternatively, one could take over and shut down the forum with hacking techniques. ¬R[provider, receiver]

The problem with this approach is that the militia can easily regroup using a secondary meeting point (for example, a pre-determined IRC channel or a website). In addition, the counterattack will likely motivate them to continue the fight, as it is now a more personal matter. Therefore, this option, while potentially the easiest to achieve, is also least likely to generate a lasting effect.

In addition, it would be possible to post messages and materials in the channel that are against the enforced laws in the jurisdiction (vs. posting attack instructions, which may be illegal but not enforced by a militia-friendly government), thus provoking a collateral response from the Internet service provider or law enforcement community.

Summary

I started this line of research in hopes of gaining a better understanding of cyber conflict and especially the role of malicious volunteer actors in it. Considering my military background, it was natural to approach the problem using the wisdom of Sun-Tzu: try to understand the adversary in order to find ways of defeating them. I believe this work is one of the first forays into the problem and that it will help others to delve deeper.

I have answered the three research questions by (a) defining the key terms in cyber conflict as part of a well founded system in Chapter 3, (b) describing the attributes, strengths and weaknesses of volunteer cyber militia groups in Chapter 4 and (c) providing ways to neutralize loosely connected cyber militias in Chapter 5. The knowledge based system of definitions described in Chapter 3 provides a convenient bridge between experts in different fields, as it is well founded and relatively straightforward. It is also applicable to other aspects of cyber conflict research, such as describing defensive organizations, discussing the effects of malware (cyber weapon), etc.

Future research

There are many ways of moving forward with this research. I will highlight the two most promising ones. The first is to continue studying the Forum type militias, as they will likely remain a wild card in international cyber conflict for some time. The Hacker Profiling Project (2009) has looked at hackers (more likely to engage in Cell type groups) in some depth using interviews and questionnaires. Considering the difficulty of gaining access to the hacking community, it should also be possible to identify, contact and interview some members of the less skilled (ad-hoc) cyber militia members.

The second promising line of research is to look at the defensive uses of volunteers. Concepts like the Estonian Cyber Defence League[16] and military reserve cyber units (for example, in UK and US) may hold the key to the national cyber defense. The benefit of such hybrid organizations is that it allows the state to benefit from the skills and expertise of volunteers in the private sector. This way, the cyber defense unit can be staffed with top experts that the government could otherwise not afford.

Regardless, I believe there is much to be learned from volunteers in cyber conflict.

[16] To be correct, the name is Estonian Defence League (EDL) Cyber Defence Unit as of 2011. See www.kaitseliit.ee for more details.

KOKKUVÕTE

Käesoleva töö inspiratsiooniks on 2007.a. kevadel Eesti vastu läbi viidud küberründed. Üldiselt aktsepteeritud narratiiv nendest sündmustest kirjeldab ründajaid kui patriootlikke häkkereid või poliitilisi (h)aktiviste, kes moodustasid ad-hoc, anonüümse ja poliitiliselt motiveeritud jõu, et rünnata sihtmärke Eestis. Kuna osa sihtmärkidest kuulusid Eesti elutähtsa taristu ja teenuste hulka, siis tõusid küberründed riikliku julgeoleku teemaks. Samas ei ole käesolevas töös käsitletav limiteeritud Eesti sündmuste kontekstiga. Sarnaseid juhtumeid on ette tulnud mitmel pool üle maailma, mistõttu võib öelda, et tegemist on ulatusliku probleemiga.

Tänu Interneti heale kättesaadavusele ning üha madalamatele oskusnõuetele infotehnoloogia kasutamisel (nt. inimene ei pea oskama lugeda, et arvutit kasutada) on küberrünnete läbiviimine tänapäeval praktiliselt kõigile jõukohane. Järelikult, sageli on vaja vaid motivatsiooni, et mingeid süsteeme rünnata. Kaitsja poolt on probleemiks, et nende ründajate tuvastamine on äärmiselt keeruline Eriti siis, kui riik, kus ründaja parajasti resideerub, ei ole huvitatud või võimeline uurijatega koostööd tegema. Isegi juhul, kui ründaja tuvastatakse, ei pruugi olla piisavalt palju tõendusmaterjali või kahju või juriidilist alust, et antud inimese vastu midagi ette võtta. Põhimõtteliselt puudub sellistel juhtudel piisav heidutus.

Antud töö arendab küberjulgeoleku uurimisvaldkonda

(a) defineerides küberkonfliktide valdkonna põhimõisted (küberrünne, küberrelv, küberkonflikt, kübersõda) fundeeritud mõistetesüsteemi osana,

(b) kirjeldades vabatahtlike küberründegruppide ja nende liikmete omadusi ja neist lähtuvaid tugevusi ja nõrkusi, ning

(c) pakkudes välja alternatiivseid lahendusi hajusalt organiseeritud küberründegruppide neutraliseerimiseks.

Tähtis alus käesoleva töö juures on infooperatsioonide ja proaktiivse kaitse alale iseloomuliku lähenemisviisi kasutamine. See võimaldab välja pakkuda ebakonventsionaalseid taktikaid juhuks, kus traditsiooniline tehnoloogiapõhine, õiguskaitse, diplomaatiline või sõjaline lähenemine ei tööta.

Töö koosneb sissejuhatusest, kirjanduse ülevaatest, süsteemse lähenemise tutvustusest, põhipanusest kolme küsimuse vastamise näol ja kokkuvõttest.

ABSTRACT

This thesis was inspired by the cyber attacks against Estonia in the spring of 2007. The prevailing narrative of the event describes the attackers as patriotic hackers or political (h)activists who formed an ad-hoc, anonymous and politically motivated force to launch cyber attacks against targets in Estonia. Since some of the targeted systems were part of Estonian Critical Information Infrastructure (CII), the cyber attacks became a national security issue. However, the subjects covered in the thesis are not limited to the event in Estonia. Similar cases of malicious activity have happened all over the world, which suggests that the issue is relevant to a broad audience.

The easy access to Internet and the lowering skill requirements associated with using information technology mean that (simpler) cyber attacks are within everyone's reach. All that is required then, is motivation to use cyber attacks against any target of choice. The problem from the defender's viewpoint is that it is very difficult to attribute such attacks, if the country they reside in is not able or willing to cooperate with the investigation. If attribution is possible, there may still not be enough evidence or damage or legal basis to take conventional law enforcement action against such individuals. Basically, there is often no effective deterrent for such activity.

This thesis develops the knowledge base of cyber security research by

(a) defining the key terms in cyber conflict (cyber attack, cyber weapon, cyber conflict, cyber war) as part of a well founded system,

(b) describing the attributes, strengths and weaknesses of three forms of volunteer cyber militia groups, and

(c) providing alternative ways to neutralize loosely connected cyber militia.

An important foundation for this thesis is the approach from the information operations and proactive defense perspective. This allows the use of unconventional tactics in cases where traditional technological, law enforcement, diplomatic or military force options are not effective.

The thesis consists of the introduction, overview of related work, overview of the systematic approach, the main contribution addressing the three research questions, and the summary.

References

Allen, P. & Demchak, C. (2003) The Palestinian-Israeli Cyberwar. *Military Review*, March-April 2003, p 52-59.

Alleyne, B. (2010) Sociology of Hackers Revisited. *The Sociologial Review* , p 1-35.

Armistead, E.L. (Ed.) (2004) *Information Operations: Warfare and the Hard Reality of Soft Power*. Potomac Books Inc.

Armistead, E.L. (Ed.) (2007) *Information Warfare: Separating Hype from Reality*. Potomac Books Inc.

Arwood, S., Mills, R. & Raines, R. (2010) Operational Art and Strategy in Cyberspace. In *Proceedings of the 5th International Conference on Information Warfare and Security*, Dayton, OH, US, 8-9 April. Reading: Academic Publishing Limited, p 16-22.

Bardin, J. (2010) *Cyber Jihadist Use of the Internet: What Can Be Done?* Whitepaper.

Bernier, M. & Treurniet, J. (2010) Understanding Cyber Operations in a Canadian Strategic Context: More than C4ISR, More than CNO. In Czosseck, C. and Podins, K. (Eds.) *Conference on Cyber Conflict. Proceedings 2010*. Tallinn: CCD COE Publications, p 227-243.

Billo, C. & Chang, W. (2004) *Cyber Warfare: an Analysis of the Means and Motivations of Selected Nation States*. Report for Department of Homeland Security.

Buzan, B., De Wilde, J., & Waever, O. (1997) *Security: A New Framework for Analysis*. Lynne Rienner Pub.

Carr, J. (2009) *Inside Cyber Warfare*. Sebastopol: O'Reilly Media.

CCDCOE. (2009) *Excerpts From Log File Analysis of the Cyber Attacks Against Estonia in the Spring of 2007*. Whitepaper.

CCDCOE. (2011) MILCW. Available at: http://www.ccdcoe.org/249.html. [Last accessed 22.03.2010]

Chiesa, R., Ducci, S. & Ciappi S. (2009) *Profiling Hackers – The Science of Criminal Profiling as Applied to the World of Hacking*. Boca Raton: CRC Press.

Cohn P. M. (1965). *Universal Algebra*. Evanston: Harper&Row.

Conti, G. & Surdu, J. (2009) Army, Navy, Air Force, and Cyber - Is it Time for a Cyberwarfare Branch of Military? In *IA Newsletter*. Vol 12, No 1.

Coram, R. (2002) *Boyd: The Fighter Pilot Who Changed the Art of War*. Boston: Little, Brown & Company.

Cornish, P., Livingstone, D., Clemente, D., Yorke, C. (2010) *On Cyber War*. Report. Available at: http://www.chathamhouse.org.uk/publications/papers/view/-/id/967/ [Last accessed 22.03.2010]

Council of Europe. (2001). Convention on Cybercrime. Available at: http://conventions.coe.int/treaty/en/treaties/html/185.htm. [Last accessed 22.03.2010]

Czosseck, C., Ottis, R. & Talihärm, A-M. (2011) Estonia 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security. Accepted for publication in the 10th European Conference on Information Warfare and Security, 7-8 July, Tallinn.

Denning, D.E. (1999) Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. Nautilus Institute. A revised version appeared in *The Computer Security Journal*, Vol. XVI, No. 3, Summer 2000, p 15-35. A further revision appeared in *Networks and Netwars : The Future of Terror, Crime, and Militancy*, J. Arquilla and D. F. Ronfeldt (Eds.), 2001, p 239-288.

Denning, D. E. (2004) *Information Warfare and Security*. Boston: Addison Wesley.

Denning, D. E. (2010) Cyber Conflict as an Emergent Social Phenomenon. In Holt, T. & Schell, B. (Eds.) *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*. IGI Global, p 170-186.

Deibert, R., Rohozinski, R. (2010) Liberation vs. Control: The Future of Cyberspace. In *Journal of Democracy*, October 2010, Vol 21, No 4, p 43-57.

Fritz, J. (2008) How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness. *Culture Mandala*, Vol. 8, No. 1, p 28-80.

Geer, D. (2010) Cybersecurity and National Policy. *Harvard National Security Journal*, Vol 1, p 207-219.

Goodman, W. (2010) Cyber Deterrence: Tougher in Theory than in Practice. In *Strategic Studies Quarterly*, Fall ed., p 102-135.

Grätzer, G. (2008). *Universal Algebra*. Second Edition. Springer.

Hartley, R. V. L. (1928). Transmission of Information. *BSTJ*, 7, 3, p 535-563.

Hare, F. (2010) The Cyber Threat to National Security: Why Can't We Agree? In Czosseck, C. and Podins, K. (Eds.) *Conference on Cyber Conflict. Proceedings 2010*. Tallinn: CCD COE Publications, p 211-225.

Hintz, A., Milan, S. (2010) Social Science is Police Science: Researching Grass-Roots Activism. *International Journal of Communication*, Vol 4, 837-844.

Huhtinen, A., Armistead, L., Schou, C. (2010) Educating and Training Soldiers for Information Operations. In *Proceedings of the 5th International Conference on Information Warfare and Security*, Dayton, OH, US, 8-9 April. Reading: Academic Publishing Limited, p 155-162.

Joint Publication 3-13. Information Operations. (2006) Chairman of the Joint Chiefs of Staff.

Karatzogianni, A. (2010) Blame It on the Russians: Tracking the Portrayal of Russian Hackers during Cyber Conflict Incidents. In *Digital Icons: Studies in Russian, Eurasian and Central European New Media*, No. 4, p 127-150.

Krekel, B., DeWeese, S., Bakos, G., Barnett, C. (2009) *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*. Report for the US-China Economic and Security Review Commission.

Lemay, A., Fernandez, J.M., Knight, S. (2010) Pinprick Attacks, a Lesser Included Case. In Czosseck, C. and Podins, K. (Eds.) *Conference on Cyber Conflict. Proceedings 2010*. Tallinn: CCD COE Publications, p 183-194.

Leaven, T., Dodge, C. (2010) The United States Cyber Command: International Restrictions vs. Manifest Destiny. *North Carolina Journal of Law & Technology*, Vol 12, online ed., p 1-28.

Liles, S. (2010) Cyber Warfare: as a Form of Low-Intensity Conflict and Insurgency. In Czosseck, C. and Podins, K. (Eds.) *Conference on Cyber Conflict. Proceedings 2010*. Tallinn: CCD COE Publications, p 47-57.

Lorents, P. (1998) *Süsteemse käsitluse alused. Riigikaitse ja julgeoleku põhiküsimused*. Tallinn: Eesti Riigikaitse Akadeemia kirjastus. [Foundations of the Systematic Approach. Main Problems of National Defence and Security]

Lorents, P. (2001a) Formalization of data and knowledge based on the fundamental notation-denotation relation. In *Proceedings of the International Conference on Artificial Intelligence. IC – AI' 2001*. Vol III, p 1297-1301.

Lorents, P. (2001b) *Informaatika teoreetilised alused. Struktuurne aspekt*. Tallinn: EBS Print. [Theoretical Foundation of Informatics. Structural Aspect]

Lorents, P. (2006) *Süsteemide maailm*. Tartu: Tartu Ülikooli Kirjastus. [The World of Systems]

Lorents, P. (2008) Knowledge and Taxonomy of Intellect. In *Proceedings of the International Conference on Artificial Intelligence. IC-AI' 2007*. Las Vegas, US, July 25-28, Vol II, p 484-489. CSREA Press.

Lynn, W.J. (2010) Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*, Sept./Oct.

Maltsev, A. I. [Мальцев А. И.] (1970). Алгебраические системы [Algebraic systems]. Moscow: Наука.

Meikle, G. (2009) Electronic civil disobedience and symbolic power. In Karatzogianni, A. (Ed.) *Cyber Conflict and Global Politics*. London: Routledge, p 177-187.

Michael, J.B., Wingfield, T.C., Wijesekera, D. (2003) Measured Responses to Cyber Attacks Using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System. In *Proceedings of the 27th Annual International Computer Software and Applications Conference, IEEE*.

Mulvenon, J. (1999) The People's Liberation Army in the Information Age. Santa Monica, CA, USA: Rand. Available at: http://www.rand.org/pubs/conf_proceedings/CF145/CF145.chap9.pdf. [Last accessed 22.03.2010]

NATO Strategic Concept. (2010) Online at: http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf [Last accessed 22.03.2010]

Nazario, J. (2009) Politically Motivated Denial of Service Attacks. In Czosseck, C. & Geers, K. (Eds.) *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam: IOS Press, pp 163-181.

Nissenbaum, H. (2005) Where Computer Security Meets National Security. In *Ethics and Information Technology*. Vol 7, No 2.

Ottis, R. (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, Plymouth*. Reading: Academic Publishing Limited, p 163-168.

Ottis, R. (2009) Konfliktid infoajastul - küberründed ja kodanikuühiskond. *Akadeemia*, Nr 9. [*Conflicts in the Information Age – Cyber Attacks and the Citizen Society*]

Ottis, R. (2010) From Pitch Forks to Laptops: Volunteers in Cyber Conflicts. In Czosseck, C. and Podins, K. (Eds.) *Conference on Cyber Conflict. Proceedings 2010*. Tallinn: CCD COE Publications, p 97-109.

Perry, W. (2007) *Information Warfare: An Emerging and Preferred Tool of the People's Republic of China*. Occasional Papers Series, Center for Security Policy.

Rattray, G. (2001) *Strategic Warfare in Cyberspace*. Cambridge: MIT Press.

Rios, B. (2009) *Sun Tzu was a Hacker: An Examination of the Tactics and Operations from a Real World Cyber Attack*. In Czosseck, C. & Geers, K. (Eds.) *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam: IOS Press, p 143-155.

Samuel, A.W. (2004) *Hactivism and the Future of Political Participation*. PhD Thesis, Harvard University, Cambridge.

Sawyer, R.D. (1994) *Sun-Tzu: The Art of War*. Boulder: Westview Press.

Schmitt, M. (1999). Computer Network Attack and Use of Force in International Law: Thoughts on a Normative Framework. In *Columbia Journal of Transnational Law*, Vol 37, p 885-937.

Schmitt, M. (2002). Wired warfare: Computer network attack and jus in bello. In *International Review of the Red Cross*, Vol 84, No 846, pp 365-399.

Schweitzer, D., Fulton, S. (2010) A hybrid Approach to Teaching Information Warfare. In *Proceedings of the 5th International Conference on Information Warfare and Security*, Dayton, OH, US, 8-9 April. Reading: Academic Publishing Limited, p 299-307.

Shackelford, S.J. (2010) State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. In Czosseck, C. and Podins, K. (Eds.) *Conference on Cyber Conflict. Proceedings 2010*. Tallinn: CCD COE Publications, p 197-208.

Shannon, C. E. (1949). Communication in the presence of noise. *PIRE*, 37, 1, p 10-21.

Starr, S., Kuehl, D., Pudas, T. (2010) Perspectives on Building a Cyber Force Structure. In Czosseck, C. and Podins, K. (Eds.) *Conference on Cyber Conflict. Proceedings 2010*. Tallinn: CCD COE Publications, p 163-181.

Thomas, T.L. (2004) *Chinese Information War Theory and Practice*. Fort Leavenworth: Foreign Military Studies Office.

Thomas, T.L. (2005) *Cyber Silhouettes*. Fort Leavenworth: Foreign Military Studies Office.

Thomas, T.L. (2007) *Decoding the Virtual Dragon*. Fort Leavenworth: Foreign Military Studies Office.

Thomas, T.L. (2008) *China's Electronic Long-Range Reconnaissance*. Military Review, November-December 2008, pp. 47-54.

Tuller, W. G. (1949). Theoretical limitations on the rate of transmissioon of information. *PIRE*, 37, 5, p 468-478.

Veerasamy, N. (2010) A High-Level Mapping of Cyberterrorism to the OODA Loop. In *Proceedings of the 5th International Conference on Information Warfare and Security*, Dayton, OH, US, 8-9 April. Reading: Academic Publishing Limited, p 352-360.

von Clausewitz, C. (1997) *On War*. Hertfordshire: Wordsworth Editions Ltd.

Warden, J.A. (1995) Air Theory for the Twenty-first Century. Schneider, B.R. & Grinter, L.E. (Eds.) *Battlefield of the Future, 21st Century Warfare Issues*. Air War College Studies in National Security, September.

Watts, S. (forthcoming) Low Intensity Computer Network Attack and Self Defense. *International Law Studies*.

West, D., Latham, C. (2010) The Extremist Edition of Social Networking: The Inevitable Marriage of Cyber Jihad and Web 2.0. In *Proceedings of the 5th International Conference on Information Warfare and Security*, Dayton, OH, US, 8-9 April. Reading: Academic Publishing Limited, p 523-531.

Wiener, N. (1948) *Cybernetics: Or Control and Communication in the Animal and the Machine*. New York: John Wiley.

Williams, G., Arreymbi, J. (2007) Is Cyber Tribalism Winning Online Information Warfare? In *Proceedings of ISSE/SECURE 2007 Securing Electronic Business Processes*. Wiesbaden: Vieweg.

Wilson, C. (2007) *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*. CRS Report for Congress.

Wilson Wrona, J-M. (2005) *From Sticks and Stones to Zeros and Ones: the Development of Computer Network Operations as an Element of Warfare*. Master's thesis, Naval Postgraduate School.

Wu, C. (2004) An Overview of the Research and Development of Information Warfare in China. In Edward Halpin et al. (eds.) (2006) *Cyberwar, Netwar and the Revolution in Military Affairs*. Palgrave MacMillan, Hampshire, pp 173-195.

Young, S., Aitel, D. (2004) *The Hacker's Handbook. The Strategy behind Breaking into and Defending Networks*. Boca Raton: Auerbach.

Yurcik, W. and Doss, D. (2001) Internet Attacks: A Policy Framework for Rules of Engagement. In *The 29th Research Conference on Communication, Information and Internet Policy*, Alexandria.

ELULOOKIRJELDUS

1. Isikuandmed
   Ees- ja perekonnanimi: **Rain Ottis**
   Sünniaeg ja -koht: **21.01.1981, Keila, Eesti**
   Kodakondsus: **Eesti**

2. Kontaktandmed
   Aadress: **Filtri 12, Tallinn, 10132**
   Telefon: **+372 717 6870**
   E-posti aadress: **rain.ottis@ccdcoe.org**

3. Hariduskäik

Õppeasutus (nimetus lõpetamise ajal)	Lõpetamise aeg	Haridus (eriala/kraad)
Unites States Military Academy	2003	Arvutiteadus/bakalaureus (Bachelor of Science in Computer Science)
Tallinna Tehnikaülikool	2007	Informaatika/tehnikateaduste magister

4. Keelteoskus (alg-, kesk- või kõrgtase)

Keel	Tase
Eesti	Kõrgtase (emakeel)
Inglise	Kõrgtase
Soome	Algtase
Saksa	Algtase
Vene	Algtase

5. Täiendusõpe

Õppimise aeg	Täiendusõppe läbiviija nimetus
2004	Signal Officer Basic Course, US Army Signal School, Fort Gordon
2005	Hands-on Hacking Course, Domina Security, Tallinn
2006	Computer Security Course, NATO CIS School, Latina

6. Teenistuskäik

Töötamise aeg	Tööandja nimetus	Ametikoht
2003-2005	Üksik-sidepataljon	Ohvitser-instruktor
2005-2008	Kaitseväe Side- ja Infosüsteemide Väljaõppe- ja Arenduskeskus (KV SIVAK)	Küberkaitse jaoskonna ülem
2008-...	NATO Kooperatiivne Küberkaitse Kompetentsikeskus	Teadur

7. Teadustegevus

Czosseck, C., Talihärm, A.M., Ottis, R. (2011) Cyber Security related Legal, Strategy and Organizational Changes in Estonia after 2007's Cyber Attacks. In *10th European Conference on Information Warfare and Security*, Tallinn. [accepted for publication]

Lorents, P. & Ottis, R. (2010) Knowledge Based Framework for Cyber Weapons and Conflict. In Czosseck, C. and Podins, K. (Eds.) *Conference on Cyber Conflict. Proceedings 2010*. Tallinn: CCD COE Publications, p 129-142.

Lorents, P., Ottis, R., Rikk, R. (2009). Cyber Society and Cooperative Cyber Defence. In *Internationalization, Design and Global Development*. *Lecture Notes in Computer Science*, Vol 5623, p 180-186.

Ottis, R. (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, Plymouth*. Reading: Academic Publishing Limited, p 163-168.

Ottis, R. (2009) Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability. In *Proceedings of the 8th European Conference on Information Warfare and Security, Lisbon*. Reading: Academic Publishing Limited, p 177-182.

Ottis, R. (2010) From Pitch Forks to Laptops: Volunteers in Cyber Conflicts. In Czosseck, C. and Podins, K. (Eds.) *Conference on Cyber Conflict. Proceedings 2010*. Tallinn: CCD COE Publications, p 97-109.

Ottis, R. (2010) Proactive Defence Tactics Against On-Line Cyber Militia. In *Proceedings of the 9th European Conference on Information Warfare and Security*, Thessaloniki. Reading: Academic Publishing Limited, p 233-237.

Ottis, R. (2011) Theoretical Offensive Cyber Militia Models. In *Proceedings of the 6th International Conference on Information Warfare and Security*, Washington DC. Reading: Academic Publishing Limited pp 307-313.

Ottis, R., Lorents, P. (2010) Cyberspace: Definition and Implications. In *Proceedings of the 5th International Conference on Information Warfare and Security*, Dayton, OH, US, 8-9 April. Reading: Academic Publishing Limited, p 267-270.

8. Kaitstud lõputööd

Analysis of the Attacker Profiles in the 2007 Cyber Attacks against Estonia. Magistritöö, Tallinna Tehnikaülikool.
[Ründeprofiilide analüüs 2007. aastal Eesti vastu sooritatud küberrünnakute põhjal]

9. Teadustöö põhisuunad

Küberkaitse riikliku julgeoleku osana, küberründed, küberkonfliktid

10. Teised uurimisprojektid

Manual on International Law Applicable to Cyber Conflict

CURRICULUM VITAE

1. Personal data
   Name: **Rain Ottis**
   Date and place of birth: **21.01.1981, Keila, Estonia**

2. Contact information
   Address: **Filtri 12, Tallinn, 10132**
   Phone: **+372 717 6870**
   E-mail: **rain.ottis@ccdcoe.org**

3. Education

Educational institution	Graduation year	Education (field of study/degree)
Unites States Military Academy	2003	Bachelor of Science in Computer Science
Tallinn University of Technology	2007	Master of Science in Engineering (Informatics)

4. Language competence/skills (fluent; average, basic skills)

Language	Level
Estonian	Fluent (native)
English	Fluent
Finnish	Basic skills
German	Basic skills
Russian	Basic skills

5. Special Courses

Period	Educational or other organisation
2004	Signal Officer Basic Course, US Army Signal School, Fort Gordon
2005	Hands-on Hacking, Domina Security, Tallinn
2006	Computer Security Course, NATO CIS School, Latina

6. Professional Employment

Period	Organisation	Position
2003-2005	Single Signal Battalion, Estonian Defence Forces	Officer-instructor
2005-2008	Estonian Defence Forces Training and Development Centre of Communication and Information Systems (EDF TDCCIS)	Chief of Cyber Defence Section
2008-present	Cooperative Cyber Defence Centre of Excellence	Scientist

7. Scientific work

Czosseck, C., Talihärm, A.M., Ottis, R. (2011) Cyber Security related Legal, Strategy and Organizational Changes in Estonia after 2007's Cyber Attacks. In *10th European Conference on Information Warfare and Security*, Tallinn. [accepted for publication]

Lorents, P. & Ottis, R. (2010) Knowledge Based Framework for Cyber Weapons and Conflict. In Czosseck, C. and Podins, K. (Eds.) *Conference on Cyber Conflict. Proceedings 2010*. Tallinn: CCD COE Publications, p 129-142.

Lorents, P., Ottis, R., Rikk, R. (2009). Cyber Society and Cooperative Cyber Defence. In *Internationalization, Design and Global Development*. *Lecture Notes in Computer Science*, Vol 5623, p 180-186.

Ottis, R. (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, Plymouth*. Reading: Academic Publishing Limited, p 163-168.

Ottis, R. (2009) Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability. In *Proceedings of the 8th European Conference on Information Warfare and Security, Lisbon*. Reading: Academic Publishing Limited, p 177-182.

Ottis, R. (2010) From Pitch Forks to Laptops: Volunteers in Cyber Conflicts. In Czosseck, C. and Podins, K. (Eds.) *Conference on Cyber Conflict. Proceedings 2010*. Tallinn: CCD COE Publications, p 97-109.

Ottis, R. (2010) Proactive Defence Tactics Against On-Line Cyber Militia. In *Proceedings of the 9th European Conference on Information Warfare and Security*, Thessaloniki. Reading: Academic Publishing Limited, p 233-237.

Ottis, R. (2011) Theoretical Offensive Cyber Militia Models. In *Proceedings of the 6th International Conference on Information Warfare and Security*, Washington DC. Reading: Academic Publishing Limited pp 307-313.

Ottis, R., Lorents, P. (2010) Cyberspace: Definition and Implications. In *Proceedings of the 5th International Conference on Information Warfare and Security*, Dayton, OH, US, 8-9 April. Reading: Academic Publishing Limited, p 267-270.

8. Defended theses

Analysis of the Attacker Profiles in the 2007 Cyber Attacks against Estonia. Master's Thesis, Tallinn University of Technology
[Ründeprofiilide analüüs 2007. aastal Eesti vastu sooritatud küberrünnakute põhjal]

9. Main areas of scientific work/Current research topics

Cyber security as part of national security, cyber attacks, cyber conflicts

10. Other research projects

Manual on International Law Applicable to Cyber Conflict

Publications

I Lorents, P. and Ottis, R. (2010) Knowledge Based Framework for Cyber Weapons and Conflict. In Czosseck, C. and Podins, K. (Eds.) *Conference on Cyber Conflict. Proceedings 2010*. Tallinn: CCD COE Publications, p 129-142.

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

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 al-

low 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 $(A \int B)$, or in simple cases as $A \int B$. The symbol "$\int$" 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 $\langle A,B \rangle$.

Note that the notation-denotation relationship "$\int$" 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 exam-

ple, (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)]:

$$\dfrac{\dfrac{}{X=Y\rightarrow Y=X}\qquad \dfrac{}{Y=X\rightarrow(Y\int X)}}{X=Y\rightarrow(X\int Y)}\qquad \dfrac{}{X=Y\rightarrow(Y\int X)}$$

$$X=Y\rightarrow(X\int Y)\&(Y\int X)$$

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 them-

selves, 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: $K \pounds W \cdot \log_2(1+P/N)$ (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 – $A \int B$.

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

- there are A and B, so that $(A \int B)$ and $X=\langle A,B\rangle$, or
- there are A and B, so that $(A \int B)$ and $X=A$, or
- there are A and B, so that $(A \int B)$ 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 $A \int B$.

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

- there is an argument "there are A and B, so that $(A \int B)$ and $X=\langle A,B\rangle$" while $A \int B$ is *not true*, or
- there is an argument "there are A and B, so that $(A \int B)$ and $X=A$" while $A \int B$ is *not true*, or
- there is an argument "there are A and B, so that $(A \int B)$ and $X=B$" while $A \int B$ 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 $(A \int B)$ and $X=\langle A,B\rangle$, or
- there are A and B, so that $(A \int B)$ and $X=A$, or
- there are A and B, so that $(A \int B)$ and $X=B$.

Theorem. X is not information, if:

- there *are no* A and B, so that $(A \int B)$ and $X= \langle A,B\rangle$, *and*
- there *are no* A and B, so that $(A \int B)$ and $X=A$, *and*
- there *are no* A and B, so that $(A \int B)$ 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 $X= \langle A,B\rangle$ 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 $X=\langle A,B\rangle$ 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. There-

fore, 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.

II Ottis, R. (2011) Theoretical Offensive Cyber Militia Models. In *Proceedings of the 6th International Conference on Information Warfare and Security*, Washington DC. Reading: Academic Publishing Limited pp 307-313.

Theoretical Offensive Cyber Militia Models

Rain Ottis
Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia
rain.ottis@ccdcoe.org

Abstract. Volunteer based non-state actors have played an important part in many international cyber conflicts of the past two decades. In order to better understand this threat I describe three theoretical models for volunteer based offensive cyber militias: the Forum, the Cell and the Hierarchy. The Forum is an ad-hoc cyber militia form that is organized around a central communications platform, where the members share information and tools necessary to carry out cyber attacks against their chosen adversary. The Cell model refers to hacker cells, which engage in politically motivated hacking over extended periods of time. The Hierarchy refers to the traditional hierarchical model, which may be encountered in government sponsored volunteer organizations, as well as in cohesive self-organized non-state actors. For each model, I give an example and describe the model's attributes, strengths and weaknesses using qualitative analysis. The models are based on expert opinion on different types of cyber militias that have been seen in cyber conflicts. These theoretical models provide a framework for categorizing volunteer based offensive cyber militias of non-trivial size.

Keywords: cyber conflict, cyber militia, cyber attack, patriotic hacking, on-line communities

1. Introduction

The widespread application of Internet services has given rise to a new contested space, where people with conflicting ideals or values strive to succeed, sometimes by attacking the systems and services of the other side. It is interesting to note that in most public cases of cyber conflict the offensive side is not identified as a state actor, at least not officially. Instead, it often looks like citizens take part in hactivist campaigns or patriotic hacking on their own, volunteering for the cyber front.

Cases like the 2007 cyber attacks against Estonia are a good example where an informal non-state cyber militia has become a threat to national security. In order to understand the threat posed by these volunteer cyber militias I provide three models of how such groups can be organized and analyze the strengths and weaknesses of each.

The three models considered are the Forum, the Cell and the Hierarchy. The models are applicable to groups of non-trivial size, which require internal assignment of responsibilities and authority.

1.1 Method and limitations

In this paper I use theoretical qualitative analysis in order to describe the attributes, strengths and weaknesses of three offensively oriented cyber militia models. I have chosen the three plausible models based on what can be observed in recent cyber conflicts. The term *model* refers to an abstract description of relationships between members of the cyber militia, including command, control and mentoring relationships, as well as the operating principles of the militia.

Note, however, that the description of the models is based on theoretical reasoning and expert opinion. It offers abstract theoretical models in an ideal setting. There may not be a full match to any of them in reality or in the examples provided. It is more likely to see either combinations of different models or models that do not match the description in full. On the other hand, the models should serve as useful frameworks for analyzing volunteer groups in the current and coming cyber conflicts.

In preparing this work, I communicated with and received feedback from a number of recognized experts in the field of cyber conflict research. I wish to thank them all for providing comments on my proposed models: Prof Dorothy Denning (Naval Postgraduate School), Dr Jose Nazario (Arbor Networks), Prof Samuel Liles (Purdue University Calumet), Mr Jeffrey Carr (Greylogic) and Mr Kenneth Geers (Cooperative Cyber Defence Centre of Excellence).

2. The forum

The global spread of the Internet allows people to connect easily and form „cyber tribes", which can range from benign hobby groups to antagonistic ad-hoc cyber militias. (Williams 2007, Ottis 2008, Carr 2009, Nazario 2009, Denning 2010) In the case of an ad-hoc cyber militia, the Forum unites like-minded people who are "willing and able to use cyber attacks in order to achieve a political goal."

(Ottis 2010b) It serves as a command and control platform where more active members can post motivational materials, attack instructions, attack tools, etc. (Denning 2010)

This particular model, as well as the strengths and weaknesses covered in this section, are based on (Ottis 2010b). A good example of this model in recent cyber conflicts is the *stopgeorgia.ru* forum during the Russia-Georgia war in 2008 (Carr 2009).

2.1 Attributes

The Forum is an on-line meeting place for people who are interested in a particular subject. I use Forum as a conceptual term referring to the people who interact in the on-line meeting place. The technical implementation of the meeting place could take many different forms: web forum, Internet Relay Chat channel, social network subgroup, etc. It is important that the Forum is accessible over Internet and preferably easy to find. The latter condition is useful for recruiting new members and providing visibility to the agenda of the group.

The Forum mobilizes in response to an event that is important to the members. While there can be a core group of people who remain actively involved over extended periods of time, the membership can be expected to surge in size when the underlying issue becomes “hot“. Basically, the Forum is like a flash mob that performs cyber attacks instead of actions on the streets. As such, the Forum is more ad-hoc than permanent, because it is likely to disband once the underlying event is settled.

The membership of the Forum forms a *loose network* centered on the communications platform, where few, if any, people know each other in real life and the entire membership is not known to any single person (Ottis 2010b). Most participate anonymously, either providing an alias or by remaining passive on the communication platform. In general, the Forum is an informal group, although specific roles can be assumed by individual members. For example, there could be trainers, malware providers, campaign planners, etc. (Ottis 2010b) Some of the Forum members may also be active in cyber crime. In that case, they can contribute resources such as malware or use of a botnet to the Forum.

The membership is diverse, in terms of skills, resources and location. While there seems to be evidence that a lot of the individuals engaged in such activities are relatively unskilled in cyber attack techniques (Carr 2009), when supplemented with a few more experienced members the group can be much more effective and dangerous (Ottis 2010a).

Since most of the membership remains anonymous and often passive on the communications platform, the leadership roles will be assumed by those who are active in communicating their intent, plans and expertise. (Denning 2010) However, this still does not allow for strong command and control, as each member can decide what, if any, action to take.

2.2 Strengths

One of the most important strengths of a loose network is that it can form very quickly. Following an escalation in the underlying issue, all it takes is a rallying cry on the Internet and within hours or even minutes the volunteers can gather around a communications platform, share attack instructions, pick targets and start performing cyber attacks.

As long as there is no need for tightly controlled operations, in terms of timing, resource use and targeting, there is very little need for management. The network is also easily scalable, as anyone can join and there is no lengthy vetting procedure.

The diversity of the membership means that it is very difficult for the defenders to analyze and counter the attacks. The source addresses are likely distributed globally (black listing will be inefficient) and the different skills and resources ensure heterogeneous attack traffic (no easy patterns). In addition, experienced attackers can use this to conceal precision strikes against critical services and systems.

While it may seem that neutralizing the communications platform (via law enforcement action, cyber attack or otherwise) is an easy way to neutralize the militia, this may not be the case. The militia can easily regroup at a different communications platform in a different jurisdiction. Attacking the Forum directly may actually increase the motivation of the members. (Ottis 2010b)

Last, but not least, it is very difficult to attribute these attacks to a state, as they can (seem to) be a true (global) grass roots campaign, even if there is some form of state sponsorship. Some states may take advantage of this fact by allowing such activity to continue in their jurisdiction, blaming legal obstacles or lack of capability for their inactivity. It is also possible for government operatives to "create" a "grass roots" Forum movement in support of the government agenda. (Ottis 2009)

2.3 Weaknesses

A clear weakness of this model is the difficulty to command and control the Forum. Membership is not formalized and often it is even not visible on the communication platform, because passive readers can just take ideas from there and execute the attacks on their own. This uncoordinated approach can seriously hamper the effectiveness of the group as a whole. It may also lead to uncontrolled expansion of conflict, when members unilaterally attack third parties on behalf of the Forum.

A problem with the loose network is that it is often populated with people who do not have experience with cyber attacks. Therefore, their options are limited to primitive manual attacks or preconfigured automated attacks using attack kits or malware. (Ottis 2010a) They are highly reliant on instructions and tools from more experienced members of the Forum.

The Forum is also prone to infiltration, as it must rely on relatively easily accessible communication channels. If the communication point is hidden, the group will have difficulties in recruiting new members. The assumption is, therefore, that the communication point can be easily found by both potential recruits, as well as infiltrators. Since there is no easy way to vet the incoming members, infiltration should be relatively simple.

Another potential weakness of the Forum model is the presumption of anonymity. If the membership can be infiltrated and convinced that their anonymity is not guaranteed, they will be less likely to participate in the cyber militia. Options for achieving this can include "exposing" the "identities" of the infiltrators, arranging meetings in real life, offering tools that have a phone-home functionality to the members, etc. Note that some of these options may be illegal, depending on the circumstances. (Ottis 2010b)

3. The cell

Another model for a volunteer cyber force that has been seen is a hacker cell. In this case, the generic term *hacker* is used to encompass all manner of people who perform cyber attacks on their own, regardless of their background, motivation and skill level. It includes the hackers, crackers and script kiddies described by Young and Aitel (2004). The hacker cell includes several hackers who commit cyber attacks on a regular basis over extended periods of time. Examples of hacker cells are Team Evil and Team Hell, as described in Carr (2009).

3.1 Attributes

Unlike the Forum, the Cell members are likely to know each other in real life, while remaining anonymous to the outside observer. Since their activities are almost certainly illegal, they need to trust each other. This limits the size of the group and requires a (lengthy) vetting procedure for any new recruits. The vetting procedure can include proof of illegal cyber attacks.

The command and control structure of the Cell can vary from a clear self-determined hierarchy to a flat organization, where members coordinate their actions, but do not give or receive orders. In theory, several Cells can coordinate their actions in a joint campaign, forming a confederation of hacker cells.

The Cells can exist for a long period of time, in response to a long-term problem, such as the Israel-Palestine conflict. The activity of such a Cell ebbs and flows in accordance with the intensity of the underlying conflict. The Cell may even disband for a period of time, only to reform once the situation intensifies again.

Since hacking is a hobby (potentially a profession) for the members, they are experienced with the use of cyber attacks. One of the more visible types of attacks that can be expected from a Cell is the website defacement. Defacement refers to the illegal modification of website content, which often includes a message from the attacker, as well as the attacker's affiliation. The Zone-H web archive

lists thousands of examples of such activity, as reported by the attackers. Many of the attacks are clearly politically motivated and identify the Cell that is responsible.

Some members of the Cell may be involved with cyber crime. For example, the development, dissemination, maintenance and use of botnets for criminal purposes. These resources can be used for politically motivated cyber attacks on behalf of the Cell.

3.2 Strengths

A benefit of the Cell model is that it can mobilize very quickly, as the actors presumably already have each other's contact information. In principle, the Cell can mobilize within minutes, although it likely takes hours or days to complete the process.

A Cell is quite resistant to infiltration, because the members can be expected to establish their hacker credentials before being allowed to join. This process may include proof of illegal attacks.

Since the membership can be expected to be experienced in cyber attack techniques, the Cell can be quite effective against unhardened targets. However, hardened targets may or may not be within the reach of the Cell, depending on their specialty and experience. Prior hacking experience also allows them to cover their tracks better, should they wish to do so.

3.3 Weaknesses

While a Cell model is more resistant to countermeasures than the Forum model, it does offer potential weaknesses to exploit. The first opportunity for exploitation is the hacker's ego. Many of the more visible attacks, including defacements, leave behind the alias or affiliation of the attacker, in order to claim the bragging rights. (Carr 2009) This seems to indicate that they are quite confident in their skills and proud of their achievements. As such, they are potentially vulnerable to personal attacks, such as taunting or ridiculing in public. Stripping the anonymity of the Cell may also work, as at least some members could lose their job and face law enforcement action in their jurisdiction. (Carr 2009) As described by Ottis (2010b), it is probably not necessary to actually identify all the members of the Cell. Even if the identity of a few of them is revealed or if the corresponding perception can be created among the membership, the trust relationship will be broken and the effectiveness of the group will decrease.

Prior hacking experience also provides a potential weakness. It is more likely that the law enforcement know the identity of a hacker, especially if he or she continues to use the same affiliation or hacker alias. While there may not be enough evidence or damage or legal base for law enforcement action in response to their criminal attacks, the politically motivated attacks may provide a different set of rules for the local law enforcement.

The last problem with the Cell model is scalability. There are only so many skilled hackers who are willing to participate in a politically motivated cyber attack. While this number may still overwhelm a small target, it is unlikely to have a strong effect on a large state.

4. The hierarchy

The third option for organizing a volunteer force is to adopt a traditional hierarchical structure. This approach is more suitable for government sponsored groups or other cohesive groups that can agree to a clear chain of command. For example, the People's Liberation Army of China is known to include militia type units in their IW battalions. (Krekel 2009) The model can be divided into two generic sub-models: anonymous and identified membership.

4.1 Attributes

The Hierarchy model is similar in concept to military units, where a unit commander exercises power over a limited number of sub-units. The number of command levels depends on the overall size of the organization.

Each sub-unit can specialize on some specific task or role. For example, the list of sub-unit roles can include reconnaissance, infiltration/breaching, exploitation, malware/exploit development and training. Depending on the need, there can be multiple sub-units with the same role. Consider the analogy of

an infantry battalion, which may include a number of infantry companies, anti-tank and mortar platoons, a reconnaissance platoon, as well as various support units (communications, logistics), etc. This specialization and role assignment allows the militia unit to conduct a complete offensive cyber operation from start to finish.

A Hierarchy model is the most likely option for a state sponsored entity, since it offers a more formalized and understandable structure, as well as relatively strong command and control ability. The control ability is important, as the actions of a state sponsored militia are by definition attributable to the state.

However, a Hierarchy model is not an automatic indication of state sponsorship. Any group that is cohesive enough to determine a command structure amongst them can adopt a hierarchical structure. This is very evident in Massively Multiplayer Online Games (MMOG), such as World of Warcraft or EVE Online, where players often form hierarchical groups (guilds, corporations, etc.) in order to achieve a common goal. The same approach is possible for a cyber militia as well. In fact, Williams (2007) suggests that gaming communities can be a good recruiting ground for a cyber militia.

While the state sponsored militia can be expected to have identified membership (still, it may be anonymous to the outside observer) due to control reasons, a non-state militia can consist of anonymous members that are only identified by their screen names.

4.2 Strengths

The obvious strength of a hierarchical militia is the potential for efficient command and control. The command team can divide the operational responsibilities to specialized sub-units and make sure that their actions are coordinated. However, this strength may be wasted by incompetent leadership or other factors, such as overly restrictive operating procedures.

A hierarchical militia may exist for a long time even without ongoing conflict. During “peacetime“, the militia’s capabilities can be improved with recruitment and training. This degree of formalized preparation with no immediate action in sight is something that can set the hierarchy apart from the Forum and the Cell.

If the militia is state sponsored, then it can enjoy state funding, infrastructure, as well as cooperation from other state entities, such as law enforcement or intelligence community. This would allow the militia to concentrate on training and operations.

4.3 Weaknesses

A potential issue with the Hierarchy model is scalability. Since this approach requires some sort of vetting or background checks before admitting a new member, it may be time consuming and therefore slow down the growth of the organization.

Another potential issue with the Hierarchy model is that by design there are key persons in the hierarchy. Those persons can be targeted by various means to ensure that they will not be effective or available during a designated period, thus diminishing the overall effectiveness of the militia. A hierarchical militia may also have issues with leadership if several people contend for prestigious positions. This potential rift in the cohesion of the unit can potentially be exploited by infiltrator agents.

Any activities attributed to the state sponsored militia can further be attributed to the state. This puts heavy restrictions on the use of cyber militia “during peacetime“, as the legal framework surrounding state use of cyber attacks is currently unclear. However, in a conflict scenario, the state attribution is likely not a problem, because the state is party to the conflict anyway. This means that a state sponsored offensive cyber militia is primarily useful as a defensive capability between conflicts. Only during conflict can it be used in its offensive role.

While a state sponsored cyber militia may be more difficult (but not impossible) to infiltrate, they are vulnerable to public information campaigns, which may lead to low public and political support, decreased funding and even official disbanding of the militia. On the other hand, if the militia is not state sponsored, then it is prone to infiltration and internal information operations similar to the one considered at the Forum model.

Of the three models, the hierarchy probably takes the longest to establish, as the chain of command and role assignments get settled. During this process, which could take days, months or even years, the militia is relatively inefficient and likely not able to perform any complex operations.

5. Comparison

When analyzing the three models, it quickly becomes apparent that there are some aspects that are similar to all of them. First, they are not constrained by location. While the Forum and the Cell are by default dispersed, even a state sponsored hierarchical militia can operate from different locations.

Second, since they are organizations consisting of humans, then one of the more potent ways to neutralize cyber militias is through information operations, such as persuading them that their identities have become known to the law enforcement, etc.

Third, all three models benefit from a certain level of anonymity. However, this also makes them susceptible for infiltration, as it is difficult to verify the credentials and intent of a new member.

On the other hand, there are differences as well. Only one model lends itself well to state sponsored entities (hierarchy), although, in principle, it is possible to use all three approaches to bolster the state's cyber power.

The requirement for formalized chain of command and division of responsibilities means that the initial mobilization of the Hierarchy can be expected to take much longer than the more ad-hoc Forum or Cell. In case of short conflicts, this puts the Hierarchy model at a disadvantage.

Then again, the Hierarchy model is more likely to adopt a "peace time" mission of training and recruitment in addition to the "conflict" mission, while the other two options are more likely to be mobilized only in time of conflict. This can offset the slow initial formation limitation of the Hierarchy, if the Hierarchy is established well before the conflict.

While the Forum can rely on their numbers and use relatively primitive attacks, the Cell is capable of more sophisticated attacks due to their experience. The cyber attack capabilities of the Hierarchy, however, can range from trivial to complex.

It is important to note that the three options covered here can be combined in many ways, depending on the underlying circumstances and the personalities involved.

Conclusion

Politically motivated cyber attacks are becoming more frequent every year. In most cases the cyber conflicts include offensive non-state actors (spontaneously) formed from volunteers. Therefore, it is important to study these groups.

I have provided a theoretical way to categorize non-trivial cyber militias based on their organization. The three theoretical models are: the Forum, the Cell and the Hierarchy. In reality, it is unlikely to see a pure form of any of these, as different groups can include aspects of several models. However, the strengths and weaknesses identified should serve as useful guides to dealing with the cyber militia threat.

Disclaimer: *The opinions expressed here should not be interpreted as the official policy of the Cooperative Cyber Defence Centre of Excellence or the North Atlantic Treaty Organization.*

References

Carr, J. (2009) *Inside Cyber Warfare*. Sebastopol: O'Reilly Media.

Denning, D. E. (2010) "Cyber Conflict as an Emergent Social Phenomenon." In Holt, T. & Schell, B. (Eds.) *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*. IGI Global, pp 170-186.

Krekel, B., DeWeese, S., Bakos, G., Barnett, C. (2009) *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*. Report for the US-China Economic and Security Review Commission.

Nazario, J. (2009) "Politically Motivated Denial of Service Attacks." In Czosseck, C. & Geers, K. (Eds.) *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam: IOS Press, pp 163-181.

Ottis, R. (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*. Reading: Academic Publishing Limited, pp 163-168.

Ottis, R. (2009) ”Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability.” In *Proceedings of the 8th European Conference on Information Warfare and Security*. Reading: Academic Publishing Limited, pp 177-182.

Ottis, R. (2010a) “From Pitch Forks to Laptops: Volunteers in Cyber Conflicts.” In Czosseck, C. and Podins, K. (Eds.) *Conference on Cyber Conflict. Proceedings 2010*. Tallinn: CCD COE Publications, pp 97-109.

Ottis, R. (2010b) “Proactive Defence Tactics Against On-Line Cyber Militia.” In *Proceedings of the 9th European Conference on Information Warfare and Security*. Reading: Academic Publishing Limited, pp 233-237.

Williams, G., Arreymbi, J. (2007) Is Cyber Tribalism Winning Online Information Warfare? In *Proceedings of ISSE/SECURE 2007 Securing Electronic Business Processes*. Wiesbaden: Vieweg. On-line: http://www.springerlink.com/content/t2824n02g54552m5/n

Young, S., Aitel, D. (2004) *The Hacker’s Handbook. The Strategy behind Breaking into and Defending Networks*. Boca Raton: Auerbach.

III Ottis, R. (2010) Proactive Defence Tactics Against On-Line Cyber Militia. In *Proceedings of the 9th European Conference on Information Warfare and Security*, Thessaloniki. Reading: Academic Publishing Limited, p 233-237.

Proactive Defense Tactics Against On-Line Cyber Militia

Rain Ottis
Cooperative Cyber Defence Centre of Excellence
rain.ottis@ccdcoe.org

Abstract: There is a developing trend of "popular" cyber campaigns that mirror political, economic or military conflicts in cyberspace. The Estonian case from 2007 showed that a whole nation-state can be affected by cyber attacks, whereas the Georgian case of 2008 is an illustration of a cyber campaign that mirrors an armed conflict. In both cases at least part of the attacks were likely committed by patriotic hackers – volunteers who use cyber attacks to take part in intra- or international conflicts. In such cyber conflicts usually only the targets are known while the aggressors remain anonymous. It is often difficult to discern where state capability ends and independent patriotic hacker groups begin. Furthermore, it is relatively easy to form a new cyber militia from people who have little prior experience with computers. I define *cyber militia* as a group of volunteers who are willing and able to use cyber attacks in order to achieve a political goal. I further define *on-line cyber militia* as a cyber militia where the members communicate primarily via Internet and, as a rule, hide their identity. What the newly-minted cyber warriors may lack in skill and resources, they can often compensate with numbers. However, even an ad-hoc cyber militia that is not under direct state control can be a useful extension of a state's cyber power. On the other hand, they can also become a threat to national security. Due to the global nature of the Internet, this threat is most likely coming from multiple jurisdictions, which limits the law enforcement or military options of the state. Therefore, other approaches should be considered. In order to understand the potential threat from cyber militias, either ad-hoc or permanent, we need to explore how they are organized. I provide a theoretical overview of a specific type of on-line cyber militia and then propose tactics to neutralize it. The tactics are based on a proactive defense posture and primarily use information operation techniques to achieve the effect from within the cyber militia itself.

Keywords: cyber conflict, cyber militia, proactive cyber defense, information operations, hactivism

1. Introduction

Over the past few decades the malicious activity in cyberspace has grown to levels, where it is now considered a national security issue. This is arguably due to the fact that computers have become nearly ubiquitous in modern societies. They are easy to use and very accessible, allowing the people to regularly communicate, learn, work and have fun in cyberspace (Ottis 2010).

On the other hand, it is now also easier to use this technology for malicious purposes. There are automated cyber attack kits, vulnerability databases and instruction manuals for conducting offensive operations in cyberspace. The skill level of the attacker today does not need to be high. On the contrary, some of the more visible attacks are often perpetrated by individuals with little or no computer training (Carr 2009).

While cyber crime continues to thrive in the quest for illegitimate income via cyberspace operations, the politically motivated attacks are becoming ever more common and visible. Many international conflicts in recent years have had a mirror campaign in cyberspace. The question that often develops is whether or not the cyber campaign is sponsored by the state(s) involved in the conflict, as the attacks usually seem to be the work of patriotic hackers. (Carr 2009, Nazario 2009)

However, it is quite possible that even without a direct command link with the state, the attackers still act according to the state's agenda. After all, the state may use this volunteer force in order to maintain deniability. The official cyber warriors (military, intelligence etc.) of the state are just one of the potential components of a national offensive cyber capability. Volunteers (patriotic hackers, hactivists) and mercenaries (criminals, commercially hired experts etc.) can augment the organic cyber capabilities of the government. (Ottis 2009)

People can also mobilize as a result of a true grass roots movement. Such independent groups could organize a cyber attack campaign as a sign of protest or to promote their views. If compared to an entity that has hidden state sponsorship, they would most likely look very similar to an outside observer. Either way, this type of on-line group can evolve into a threat beyond mere inconvenience as seen in cases like the Estonian and Georgian cyber conflicts. (Ottis 2008, Carr 2009, Nazario 2009, Denning 2010)

In order to cope with this threat, we must first understand how it works. Therefore, I will provide a theoretical overview of the organizational aspects of non-state political activist groups who use cyber attacks and then look at some tactics to counter these groups.

2. On-line cyber militia

Denning (2010) describes three categories of non-state attackers (separate from the ordinary cyber criminal): patriotic hackers, electronic jihadists and hactivists. The main difference among them is the choice of targets, although Denning admits that they could all be lumped together as hactivists. For the purposes of this research, however, this distinction does not matter, as the focus is on how they are organized, not who they are fighting for or against. In particular, I am interested in finding potential weaknesses in the organization and operation of cyber militias.

Let us define *cyber militia* as a group of volunteers who are willing and able to use cyber attacks in order to achieve a political goal. Let us further define *on-line cyber militia* as a cyber militia where the members communicate primarily via Internet and, as a rule, hide their identity (for example, by using a hacker alias). Cyber militias can be ad-hoc (gathering only for a specific occasion) or permanent.

The word "volunteers" in the definition refers to people who participate in the cyber militia of their own free will. They do not get paid for their activities, nor do they have a contractual obligation to the militia. They have the right to choose their level of commitment and to leave the militia, if and when they wish. Therefore, volunteer soldiers who join a government run cyber attack unit are not considered a cyber militia.

The word "political" in the definition refers to all aims that transcend the personal interest of the volunteer. This includes religious views, nationalistic views, opinions on world social order etc.

In the context of this analysis, I am focusing on a subset of on-line cyber militias that meet the following criteria:

- The communication within the militia is centralized
- There is no direct state support or control of the militia
- The members are loosely connected in real life

The centralized communication constraint is a fairly standard arrangement for communicating, preparing, planning and coordinating a cyber attack campaign of the cyber militia. Perhaps the most used communication channels are on-line forums and instant messaging services. (Carr 2009, Denning 2010) This is also very useful for the defending side, especially for observing, infiltrating and neutralizing the cyber militia.

A cyber militia that receives direct support or instructions from the government should be considered as an organic component of the state and is therefore outside the scope of this research. However, indirect or covert state support or control (as long as it is not well known among the militia) remains still in the area of interest.

Although the leadership or core group in a militia probably is personally acquainted, as a whole the members of the on-line cyber militia are loosely connected in real life. In this case loosely connected means that most members know no or few other members and nobody knows the entire membership in person. This requires them to communicate over the Internet and coincidentally makes them more susceptible to information operations techniques. While this constraint is not true in every case, it should be a safe assumption in large (numbering in the hundreds) militias and can also hold in smaller organizations.

From the forum posts it should be possible to identify the roles of the people in the cyber militia. Key "officer" roles include leaders, trainers, suppliers, while the rest could be categorized as soldiers, and "camp followers". The leaders provide motivation for action, coordination of effort and direction of attacks. The trainers provide instructions for reconnaissance, attack and covering tracks. Suppliers provide tools, such as scanners, attack kits and malware. Soldiers participate actively in the attacks, but can be expected to remain relatively passive on the forum, potentially reporting attack results or targeting information. Camp followers read the forum for their own interest, but do not participate in

the planning or execution of attacks. Identifying the different roles in the organization offers individual targeting opportunities as well as potential avenues for infiltration.

Since the cyber militia is not necessarily a formal organization, the same person may have several roles, which can change over time. It is also important to note that an "officer" role is often not appointed by the militia, but acquired by the member by actively participating in the activities.

3. Neutralizing an on-line cyber militia

Assuming that on-line cyber militias can be a considerable threat to national security, there should also be ways of neutralizing this threat. Using traditional law enforcement methods or military force is often not feasible, because personal attribution is seldom achieved and the militia members can reside in a number of different unfriendly and uncooperative jurisdictions. Therefore I will consider alternative tactics of neutralizing an on-line cyber militia. In particular, I will propose options from the strategic starting point of information operations and proactive defense.

An important caveat here is that I do not presume universal legality of any of the tactics. It would be very difficult to do, given that the legal status of the cyber militia and its actions may vary greatly, depending on the case. For example, the cyber militia may act completely within the legal framework of the host state. On the other hand, militia members could be considered illegal combatants who may be targeted for military action (Schmitt 2002). Therefore, the tactics below should be considered as theoretical options only, not as a policy manual for dealing with a cyber militia.

There are two points where the activity of an on-line cyber militia is potentially visible for observation. First, there are the logs at the targeted sites. Second, the shared communication channel (a forum, for example) where they gather, exchange opinions and plan their activities. The two places where the militia is visible are also the places where one can fight them.

Sun-Tzu said: ”Thus the highest realization of warfare is to attack the enemy’s plans; next is to attack their alliances; next to attack their army; and the lowest is to attack their fortified cities" (cited in Sawyer 1994). I will use this principle as a loose framework for considering tactics. The analogies do not need to be an exact fit and should be interpreted liberally. First, I will look at how to neutralize the militia's ability to plan and coordinate attacks. Second, I will look at ways of attacking the virtual alliances between the members that make up the cyber militia. Third, I will look at neutralizing the effectiveness of the militia's cyber attacks. Last, I consider a counter-attack against the actual communication service that is the heart of the militia's operations.

It is important to note that for the countermeasures to work, it is necessary to gain access to the main communication channel of the militia. This may be as simple as monitoring a public forum, but a more likely scenario would require at least some form of infiltration into the channel. The infiltration does not need to be very deep - a "soldier" level access would likely be sufficient to gather the necessary information about the militia. Infiltration is required, because any sufficiently mature cyber militia will likely try to hide or protect itself from outside entities. For example, the StopGeorgia.ru forum blocked US-based IP addresses to stop researchers from accessing the forum during ten days in August of 2008 (Carr 2009).

3.1 Attacking plans

One way to neutralize the militia can be called *poisoning the well* tactic. It refers to corrupting the shared communication channel with de-motivational posts, self-destructive or ineffective attack tools and methods, bad targeting data, etc. As a result, the channel loses its effectiveness as a means for coordinating the actions of the militia, the members grow frustrated with apparent lack of coherence, and the aggression gets released inside the militia in the form of angry debate. If the militia is perceived as ineffective by the members, it will eventually disband.

An alternative approach would be to hijack the militia by shifting the debate to attacking other targets. This would basically deflect the blow from the original target, making it safe.

Yet another approach is to carry out an attack in the name of the militia against a powerful third entity in order to provoke a counterstrike against the entire militia (a false flag attack). In other words, pull a

strong opponent into the fight, forcing the militia into defensive positions. As a result, the militia will have to drop its plans for the original target.

3.2 Attacking alliances

Presumably, members of the militia want to remain *anonymous* and would leave or become inactive if there was a serious chance of being personally identified. This presents another opportunity to disband the militia from within by breaking the virtual alliances between militia members.

Without attribution there can be no personal consequences. On the other hand, if the anonymity is lost (or perceived lost by the membership), the militia will lose its trustworthiness. As a result, the militia will either disband or search for an alternative (clean) communication channel. However, since the infiltrated agents will also move over to the new channel, it would only be a temporary solution.

The question is, then, how to identify the members of the forum. In reality, it is probably not necessary to identify all or even most of the members. Most likely it is enough to break the cover of one or a few people, in order to create mistrust and fear of real life consequences in a considerable portion of the membership.

There are many ways to potentially achieve attribution of a few individuals. The simplest is to "break the cover" on infiltrated agents (can use fake identities, as they would be difficult to verify by other members) and have them "confirm" it. Another is to offer attack tools to the forum that provide the information that is necessary for personal attribution (basically a Trojan). Yet another is to correlate target log data with forum posts, and go through the legal channels. Of course, attribution may be achieved by simply arranging a meeting in real life.

Note that it may not be necessary to actually follow up the attribution with legal or military action. Just posting the personal details of some users on the forum could be enough to make a considerable portion of the members leave.

3.3 Attacking the army

The loose analogy to an army in this case could be the cyber attacks organized by the militia (the soldiers that have marched to the city gates). Obviously, the defensive actions at the target come from the long list of standard cyber security measures. However, these can be deployed much more effectively, if the infiltrated agent can relay the attack plans to the defenders. Knowing when, where and how the attack will come makes the work of defenders much easier and blunts the effectiveness of the attackers. This, in turn, may have a demoralizing effect on the militia.

3.4 Attacking fortified cities

If we take the forum to be the fortified city that serves as a home base for the cyber militia, then obviously there are ways of attacking it. Conceptually the easiest would be to use law enforcement to have it taken down, or if that fails, launch a denial of service attack against the server that hosts the service. Alternatively, one could take over and shut down the forum with hacking techniques. The problem with this approach is that the militia can easily regroup using a secondary meeting point (for example, a pre-determined IRC channel or a website). In addition, the counterattack will likely motivate them to continue the fight, as it is now a more personal matter. Therefore, this option, while potentially the easiest to achieve, is also least likely to generate a lasting effect.

In addition, it would be possible to post messages and materials in the channel that are against the enforced laws in the jurisdiction (vs posting attack instructions, which may be illegal but not enforced by a militia-friendly government), thus provoking a collateral response from the Internet service provider or law enforcement community.

4. Limitations and future research

All views in this work are attributed to the author and should not to be considered as the views or policy of the Cooperative Cyber Defence Centre of Excellence or the North Atlantic Treaty Organization.

The analysis of the on-line cyber militia is based on existing literature and provides only a theoretical viewpoint to the problem area. It is a generalized model, which may not apply to all cases.

The outlined tactics are a blend of information operation techniques and offer a more proactive defense posture against an on-line cyber militia. However, depending on the case, they may contain elements that can be considered against the law. Issues that may arise include perfidy, freedom of speech, computer crime, illegal surveillance and personal data protection, to name a few. Therefore, it should not be viewed as a policy manual, but a theoretical overview of alternative tactics.

One way to move this research forward is to use social network analysis on cyber militia forum logs to identify the roles and interactions of key actors in cyber militia. This could help develop a better model for a generic cyber militia and a more detailed method for targeting key members in the militia.

5. Conclusion

The rising trend of politically motivated cyber attacks by non-state actors has changed the balance of power in cyberspace. On-line cyber militia is a type of organization that allows everyone with a computer and an Internet connection to become active in the world of cyber conflict.

Since on-line cyber militias have shown the capability to become a threat to national security, it is important to study them. I have given a theoretical overview of a specific type of cyber militia, which relies on a mass of anonymous members for its "firepower". More importantly, I have provided some generic tactics for neutralizing the on-line cyber militia, under the strategic approach of information operations and proactive defense.

References

Carr, J. (2009) *Inside Cyber Warfare*, Sebastopol, CA: O'Reilly Media.

Denning, D. E. (2010) “Cyber Conflict as an Emergent Social Phenomenon”, *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (Hold, T. & Schell, B. eds.), IGI Global. [to appear]

Nazario, J. (2009) "Politically Motivated Denial of Service Attacks*", The Virtual Battlefield: Perspectives on Cyber Warfare* (Czosseck, C. & Geers, K. eds.), Amsterdam: IOS Press, pp 163-181.

Ottis, R. (2008) “Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective”, *Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth*, Reading: Academic Publishing Limited, pp 163-168.

Ottis, R. (2009) "Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability." *Proceedings of the 8th European Conference on Information Warfare and Security, Lisbon*, Reading: Academic Publishing Limited, pp 177-182.

Ottis, R. and Lorents, P. (2010) "Cyberspace: Definition and Implications." *Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, US*. [accepted for publication]

Schmitt, M. (2002) ”Wired Warfare: Computer Network Attack and International Law”, *International Review of the Red Cross*, Vol 84, No 846, pp 365-399.

Sawyer, R.D. (1994) *Sun-Tzu: The Art of War*, Boulder: Westview Press.

IV Ottis, R., Lorents, P. (2010) Cyberspace: Definition and Implications. In *Proceedings of the 5th International Conference on Information Warfare and Security*, Dayton, OH, US, 8-9 April. Reading: Academic Publishing Limited, p 267-270.

Cyberspace: Definition and Implications

Rain Ottis and Peeter Lorents
Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia
rain.ottis@ccdcoe.org
peeter.lorents@ccdcoe.org

Abstract: In recent years the term "cyber" has been used to describe almost anything that has to do with networks and computers, especially in the security field. Another emerging field of study is looking at conflicts in cyberspace, including state-on-state cyber warfare, cyber terrorism, cyber militias etc. Unfortunately, however, there is no consensus on what "cyberspace" is, let alone what are the implications of conflicts in cyberspace. In order to clarify this situation, we offer the following definition: *cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems*. We describe the background of the definition and show why this approach may be preferable over others. Specifically, we revisit the terms coined by Norbert Wiener (the father of cybernetics) and William Gibson. We show that time-dependence is an overlooked aspect of cyber space and make a case for including it in our proposed definition. In addition, we look at the implications that can be drawn from the time-dependence of cyberspace, especially in regard to cyber conflicts, which we define as *a confrontation between two or more parties, where at least one party uses cyber attacks against the other(s)*. Specifically we review the implications on the potential for rapid deployments of offensive and defensive actions in cyberspace, the feasibility of mapping cyberspace, and the need for constant patrolling and reconnaissance.

Keywords: Cyberspace, cyber conflicts, cyber attacks, time, definition

1. Introduction

Every once in a while a new term comes along or an old term gets a novel meaning and suddenly it is everywhere. In recent years (decades, arguably), the word "cyber" has been added to a long list of words to create "new" terms. Examples of terms that surface in academic papers include cyber society (Lorents 2009), cyber attacks (Ottis 2008), offensive cyber capability (Ottis 2009), cyber defense, cyber warfare, cyber crime, cyber terrorism, etc. They all have something to do with the concept of *cyberspace*, which is often the presumed context or environment for the cyber concept in question. It follows that it is very important to have a good definition for cyberspace or the derived terms may become meaningless or flawed.

Below we review the origins of the term cyberspace and look at some of the definitions offered for it today. Following the quick overview, we propose our own definition and explain why it may be preferable over others. We finish by drawing some implications from our definition in regards to conflicts in cyberspace.

2. Overview of definitions

The term *cyber* has evolved from the work of Norbert Wiener, who defined the term *cybernetics* in the title of his book as "*control and communication in the animal and the machine*" (Wiener 1948). The idea that humans can interface with machines and that the resulting system can provide an alternative environment for interaction provides a foundation for the concept of cyberspace.

In the early 1980's the science fiction author William Gibson took the next step by coining the word *cyberspace* in one of his books. Even though this happened in a fictional setting, the word has become widely used in professional and academic circles. In his book, he described cyberspace as a "consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity." (Gibson 1984) This definition focuses on the human perception of the new environment, but is still very relevant, as it illustrates the potential for developing a truly immersive cyberspace experience. The second half of the definition identifies complexity as one of the principle characteristics of cyberspace.

Over the years, many different definitions have evolved for cyberspace. The US Department of Defense, for example, considers cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." (JP 1-02) This definition is remarkable as it only refers to the (hardware) technology

component, although software and data may be inferred from the wording. Noticeable is the lack of the human component, which is so important in Wiener's and Gibson's definitions.

The European Commission, on the other hand, vaguely defines cyberspace as "the virtual space in which the electronic data of worldwide PCs circulate". (European Commission) Again, no reference is made to the human component while the technological component is restricted to data passing between personal computers. Arguably, online encyclopedias are a more likely source of definitions for the average "citizen" of cyberspace. Webopedia, for example, offers a definition similar to the previous one, claiming that cyberspace is a "metaphor for describing the non-physical terrain created by computer systems". (Webopedia) Even though they are similar, their usefulness is limited because of vague terminology and concepts.

The Wikipedia, however, offers that cyberspace "is the global domain of electromagnetics as accessed and exploited through electronic technology and the modulation of electromagnetic energy to achieve a wide range of communication and control system capabilities." (Wikipedia) Here we have a definition that includes the technology component, the human component (who accesses and exploits) and the communication and control component, which brings us back to Norbert Wiener's definition of cybernetics.

Indeed, the variety seen in the definitions can be explained by the different viewpoints of the sources. As Strate (1999) illustrated, there is a rich taxonomy for describing cyberspace. He divided it into three tiers: zero order (ontology and cyberspacetime), first order (physical, conceptual and perceptual cyberspace) and second order cyberspace (synthesis of cybermedia space).

Even though there is a wide range of definitions from dictionary answers to state-approved terms to from-the-hip personal favorites, they mostly agree that the core of cyberspace consists of the globally connected networks of hardware, software and data. Another important aspect, which is usually not explicitly stated but can be inferred, is that humans can interface (although clumsily) with cyberspace and in doing so, become part of it. However, in order to better describe the notion of cyberspace and understand the complexity that comes with it, we must also take into account the time factor.

Time is notably absent from most definitions of cyberspace. A counterexample of this trend is the concept of cyberspacetime, which expands on the cyberspace term. "Cyberspacetime is the totality of events involving relationships between humans and computers, between humans through computers, and between computers themselves." (Strate 1999) For our purposes, however, this does not address the dynamic nature of cyberspace, but seems to encompass the entire history of events in cyberspace in one giant static setting. Therefore, we propose our own definition for cyberspace.

3. Proposed definition

As the overview of definitions showed, there is no common definition for cyberspace and the ones that are used are often vague or missing key components. We have also identified that the definitions do not properly address the dynamic nature of cyberspace. In order to correct this we propose the following definition: *cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems*.

By interconnected information systems we mean the information (Lorents 2009), hardware, software and the media that connects them. A convenient way to model such systems is to use graphs, where nodes represent computers, networking devices, sensors, user interfaces etc. and edges represent connections between nodes (cables, radio links, etc.).

Note that we have also included the human users in the definition. Cyberspace is an artificial space, created by humans for human purposes. Without human users cyberspace would stagnate, fall into disrepair and eventually – cease to be. Unless something else can take over the maintenance and development of cyber infrastructure and content, the human remains an important part of cyberspace.

Considering the amount of nodes in the global network, it becomes clear why cyberspace is considered "unthinkably complex". The International Telecommunication Union estimates that nearly a quarter of the world's population is using Internet, while over 60% are using mobile phones (ITU 2009). Supporting the user side is the core infrastructure of the networks, as well as the myriad service providers that allow people to communicate, shop, play, work – to live online.

However, the complexity increases even further if you consider that this network is not static. To highlight this issue, we have introduced the concept of *time-dependence* to our definition. Both elements and relations between elements can change (or remain unchanged) in time-dependent sets and systems as the time progresses (Lorents 2001). In cyberspace, this means that users, nodes and connections can appear and disappear, and information is transformed over time. Compared to other time-dependent systems, dramatic changes can take place in extremely short time in cyberspace. For example, a piece of malicious code can replicate, infect and effectively disable large parts of a global network in a matter of seconds or minutes.

The overview focused on the cyber part of cyberspace, but the second part of the term cyberspace – "space" – also requires some clarifying remarks. In exact and engineering sciences a space is not just any set of objects. In order to call something a space we must define the corresponding topology or metric (Kuratowski 1966). In the latter case it must be clear how the distance between elements is calculated, so that the metrics axioms are met (Deza 2006). It should be noted that several different metrics can be used on the same set of elements if the respective different distance calculation procedures are used.

It follows that there are many options for calculating distance in cyberspace. Without delving into the mathematical details, we note that in case of information systems, the "geographical" distance between nodes is probably not the most useful metric, especially considering the speed of information propagation in the system. Instead, considering that cyberspace can be modeled as a graph, we can use metrics from graph theory. For example, *distance between two nodes = shortest path between the two nodes* (Deza 2006).

4. Implications

Whether we consider cyberspace as an actual space or just a collection of resources, the actors in cyberspace (including states, businesses, organizations, groups and individuals) will compete for the control of it. As any space, cyberspace is also contested "ground", which leads us to the inevitability of conflicts in cyberspace. Let us define a cyber conflict as *a confrontation between two or more parties, where at least one party uses cyber attacks against the other(s)*. The nature of the conflict will differ based on the nature and goals of the participants. Criminals look for illegal revenue, so they hijack parts of cyberspace. Intelligence services look for useful information, so they attack enemy, friendly, or neutral parts of cyberspace to get access to that information. Militaries look to disrupt the operations of the enemy, so they attack the sensor, logistics, communications and control systems in enemy cyberspace. The conflicts can be as simple as civil disputes over domain name ownership or as complex as deliberate cyber attack campaigns as part of a conventional war between technologically advanced states.

Given the assumption that cyber conflicts are inevitable, we can draw several implications from the time-dependent aspect of cyberspace. The time-dependence is easiest to explain as *the change in the structure and content of cyberspace over time*. We have already pointed out that in cyberspace, the relevant time span can be relatively short – minutes, often even seconds or fractions of a second. Based on this we can draw implications on the potential for rapid deployments of offensive and defensive actions, the feasibility of mapping cyberspace, and the need for constant patrolling and reconnaissance. The quick changes in cyberspace imply that a relatively short amount of time is needed to carry out an attack or implement new defenses, compared to physical space. A self-replicating network worm can infect large parts of cyberspace in a matter of minutes. For example, in 2003 the SQL Slammer worm infected approximately 90% of the vulnerable hosts connected to Internet in just 10 minutes, to a total of about 75 thousand machines across all continents (Moore 2003). The only comparison to this in physical space is the simultaneous launch of hundreds or thousands of ballistic missiles armed with conventional warheads. Anything short of that will not have global consequences within a similar time span.

On the defensive side, in cyberspace it is possible to upgrade defenses in seconds or minutes by implementing new firewall rules, for example. Building a new concrete bunker or a Maginot line in physical space is much more time consuming. This does not mean that erecting defenses in cyberspace is or can always be done in minutes, however. It merely points out that it is possible to deploy prepared defensive measures (tighter firewall rules, alternative routing and hosting etc.) in a short amount of time. In preparing for a cyber conflict it is necessary to be aware of the "terrain" of the potential conflict zone, the defensive and offensive capabilities of the actors and the possibility for

collateral damage and unplanned escalation. Due to the nature of cyberspace, this is difficult to do, as the environment is complex and in constant change. Potential entry vectors, critical targets, key users and information can change within seconds. As a result, the map can only be near real-time at best and there is no way of ensuring that it will look the same on the day of the planned attack (or defense). Based on this we can draw another implication. If the map is constantly changing, then "patrolling" and reconnaissance efforts must also be constant, as long as one is concerned about the possibility of a conflict in cyberspace. This means regular monitoring and entrapment operations on the defensive side and regular probes on the offensive side. Without it, an attack may go undetected or, in the offensive case, the attack may be thwarted by a simple change in target posture. This need for constant activity, however, raises the risk of detection for the attackers and it can betray the plans and routines of the defenders.

Conversely, fire-and-forget or deploy-and-forget type attacks and defenses quickly lose their effectiveness in cyberspace, as the opposing side reacts and adapts. As is true in maneuver warfare, an obstacle is not *really* an obstacle, unless it is covered by observation and fire. Similarly, if one does not upgrade one's weapons, they will soon be unable to penetrate the armor of the enemy. Therefore, cyberspace requires constant vigilance from the planners and combatants. Many of the examples above use analogies to explain the difference or similarity between conflicts in cyberspace and physical space. These are meant to serve as illustrations only and should be treated with some reservations. The potential problems with using and abusing metaphors and analogies in cyber topics have been demonstrated by Sulek and Moran (2009).

5. Conclusion

We have given a short overview and analysis of the evolution and common meaning of the term cyberspace and made a contribution by offering a new definition. We propose that *cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems*, where the addition of time-dependence is our contribution. We have also tried to analyze the implications of the time-dependence issue from a cyber conflict perspective. While this new definition does not necessarily replace any pre-existing definitions, we feel that it does offer an important viewpoint to cyberspace that is often not considered.

References

Deza E. and Deza M.M. (2006) *Dictionary of Distances*. Amsterdam, Elsevier.

Gibson, W. (1984) *Neuromancer.* New York, Ace Books.

European Commission. "Glossary and Acronyms (Archived)". In Information Society Thematic Portal, [online], http://ec.europa.eu/information_society/tl/help/glossary/index_en.htm#c. [Accessed 03 Nov 2009]

International Telecommunication Union. (2009) "Measuring the Information Society". [online], http://www.itu.int/ITU-D/ict/publications/idi/2009/material/IDI2009_w5.pdf. [Accessed 03 Nov 2009]

Joint Publication 1-02. Department of Defense Dictionary of Military and Associated Terms. (2009) [online], http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf. [Accessed 03 Nov 2009]

Kuratowski K. (1966) *Topology*. New York, Academic Press.

Lorents, P. (2001) *Informaatika teoreetilised alused* (Theoretical Foundations of Informatics). Tallinn, EBS Print.

Lorents, P. and Ottis, R. and Rikk, R. (2009) "Cyber Society and Cooperative Cyber Defence". In *Internationalization, Design and Global Development*. Lecture Notes in Computer Science, vol. 5623, pp. 180-186.

Moore, D. and Paxson, V. and Savage, S. and Shannon, C. and Staniford, S. and Weaver, N. (2003) "Inside the Slammer Worm". *IEEE Security and Privacy,* Vol 1, No 4, pp. 33-39.

Ottis, R. (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*, Plymouth. Reading, Academic Publishing Limited, pp 163-168.

Ottis, R. (2009) "Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability." In *Proceedings of the 8th European Conference on Information Warfare and Security*, Lisbon. Reading, Academic Publishing Limited, pp 177-182.

Strate, L. (1999) "The Varieties of Cyberspace: Problems in Definition and Delimitation." *Western Journal of Communication*, Vol 63, No 3, pp. 382-412.

Sulek, D. and Moran, N. (2009) "What Analogies Can Tell Us About the Future of Cybersecurity". In Czosseck, C. and Geers, K (eds.) *The Virtual Battlefield: Perspectives on Cyber Warfare.* Amsterdam, IOS Press, pp. 118-131.

Webopedia. "cyberspace". [online], http://www.webopedia.com/TERM/c/cyberspace.html. [Accessed 03 Nov 2009]

Wiener, N. (1948) *Cybernetics: Or Control and Communication in the Animal and the Machine.* New York, John Wiley.

Wikipedia. "Cyberspace". [online], http://en.wikipedia.org/wiki/Cyberspace. [Accessed 03 Nov 2009]

V Lorents, P., Ottis, R., Rikk, R. (2009). Cyber Society and Cooperative Cyber Defence. In *Internationalization, Design and Global Development*. *Lecture Notes in Computer Science*, Vol 5623, p 180-186.

Cyber Society and Cooperative Cyber Defence

Peeter Lorents[1], Rain Ottis[1], and Raul Rikk[2]

[1] Cooperative Cyber Defence Centre of Excellence, Filtri 12, 10132 Tallinn, Estonia
[2] General Staff of Estonian Defence Forces, Juhkentali 28, 15007 Tallinn, Estonia
{Peeter.Lorents,Rain.Ottis}@ccdcoe.org,
Raul.Rikk@mil.ee

Abstract. Emergence of cyber societies places new emphasis on the protection of information and information services. The paper provides a definition for the concept of information that is based on the concept of knowledge and a definition for cyber society, which encompasses the relationship between a society of humans and a network of computers. Estonia and the cyber attacks of spring 2007 are briefly examined as an example of an early cyber society under cyber attack. Finally, the role and principles of the Cooperative Cyber Defence Centre of Excellence are explained.

Keywords: Knowledge, information, cyber society, cyber attacks, cooperative cyber defence, CCD COE.

1 Introduction

When talking about cyber society and all that it implies (including vulnerability, threats, defense etc.) it is important to clearly define *cyber society*, a term that differs from information society, IT-society, e-society etc. Without diluting our focus by comparing all the various opinions on the subject (although, see [1] for some key points) we identify aspects that describe what could be called a cyber society:

- information's importance is equivalent to traditionally valued concepts, such as energy, money etc.
- information is transmitted, processed, stored etc. on mostly computer-based systems (including universal, specialized, miniature computers etc.)
- computers are used to govern the society.

Based on the above we get to the following definition:

Definition 1. A cyber society is a society where computerized information transfer and information processing is (near) ubiquitous and where the normal functioning of this society is severely degraded or altogether impossible if the computerized systems no longer function correctly.

Following this definition, cyber society is an advanced form of human-computer interaction. This relationship (human-computer interaction) involves not just a single human and a single computer, but encompasses the relationship between a society of humans and a network of computers.

N. Aykin (Ed.): Internationalization, Design, LNCS 5623, pp. 180–186, 2009.

In order to fully understand a cyber society, including its strengths and weaknesses, we must first understand the concept of information. We will begin by defining information and other necessary concepts. Then we focus on the Republic of Estonia as an example of an early cyber society. We will also provide a short overview of the cyber attacks against Estonia that took place in the spring of 2007 and provide some lessons learned from this experience. Finally, we will discuss the principles, structure and areas of activity of the Cooperative Cyber Defence Centre of Excellence, which received its NATO accreditation in 2008.

2 Information and Information Corruption

One of the instruments for understanding various objects and processes in the world is "finding" and formally describing the relationships between them. Unfortunately, relationships come in two categories:

- Relationships that can be defined (including definitions using other relationships)
- Relationships that cannot be defined

The last types of relationships are called *fundamental relationships*.

Example. In set theory (see [2] and [3]) the concept of *being an element of* is a fundamental relationship, which is designated with a stylized "e" or the symbol "$\in$". On the other hand, the concept of *being a subset of* (designated with the symbol "$\subseteq$") is not a fundamental relationship, since it can be defined with the concept of *being an element of,* among other things (one set is a subset of another set, if every element of the first set is also an element of the second set).

In this paper we rely on the fundamental relationship of notation-denotation (see [4]), which is designated by a stylized letter "s" or the symbol "$\int$". If some objects A and B have this relationship, then A is the notation for B and B is the denotation for A. Let us agree that if we have formed an *ordered pair* of A and B, where A is the first element and B is the second element then we write this down as $\langle A,B\rangle$.

Definition 2. We call an ordered pair $\langle A,B\rangle$ *knowledge*, if A is the notation (symbol) for B and B is the denotation (meaning) for A. [4]

Note. A and B constitute knowledge, if they have the notation-denotation relationship "$\int$" or if $A \int B$.

Often knowledge is represented in text form, but not always.

Example 1. $\langle\pi$, ratio of a circle's circumference to its diameter$\rangle$ is knowledge, because $\pi \int$ *ratio of a circle's circumference to its diameter.*

Example 2. $\langle$the diagonal of a square, a straight line joining the opposite corners of a square$\rangle$ is knowledge, because *the diagonal of a square* $\int$ *a straight line joining the opposite corners of a square.*

Example 3. A red traffic light is the notation for a prohibition for moving forward. This piece of knowledge (where the color of the traffic light is the notation and the corresponding meaning is the denotation) is necessary for anyone navigating city streets.

Example 4. Hoisting the flag upside down signals distress. Unfortunately, not many are aware of this piece of knowledge, where the "wrong position" of the flag is the notation and the emergency is the denotation.

Definition 3. D is data, if there is such an A, where ⟨A,D⟩ is knowledge, or if there is such a B, where ⟨D,B⟩ is knowledge. [5]

Example. The question – what is the air temperature in the coming days – is answered by a list of numbers. Therefore, the numbers constitute data that is the *denotation* (meaning) of the words "air temperature in the coming days". The question – what do you call the country that shares a land border with only Latvia and Russia – can be answered as "Estonia", "Eesti", "Viro" etc. Therefore, in this case all these words are a *notation* (symbol) for the same country.

Note. In order to have data it is necessary to have the corresponding knowledge. If, for some X nobody knows, has known and will never know, what is the notation or denotation of X, then X *is not* data!

Definition 4. *Information,* or more shortly *info*, is either knowledge or data.

According to the definition, only one that has knowledge or data also has information. If someone holds some X, which is not knowledge or at least part of knowledge (an object in the form of a notation or a denotation), then X is not information. Following the definition the information can be corrupted by using one or more of the three main options:

- corrupt the notation;
- corrupt the denotation;
- corrupt the relationship between notation and denotation.

Depending what operations are done with the information (see [5]) – for example, transmission, storage, manipulation, systematization, destruction etc. - a suitable method can be found to corrupt the operation (which can bring about, but does not require, the corruption of the information itself). For example, enough extra information can be "pumped into" the information transmission channels that the *transmission speed* of the necessary information becomes intolerably slow. In order to corrupt a database or knowledge base it is enough to corrupt the *system*, which can be realized by deleting the data within. A more sophisticated way to corrupt a system would employ moving the data or changing the relationships between data objects etc.

3 Estonia as an Example of an Early Cyber Society

According to the definition in the introduction, a cyber society is based on ubiquitous computing and that a loss of these computer services directly affects the normal existence of this society. Computing deals with manipulating information (knowledge and data) for the benefit of the user. For example, the concept of money no longer requires a physical entity (coins, bills) that can be passed between transaction parties (from one wallet to another). Instead, the passage of wealth can be represented with a simple change of numbers in the related accounts (stored in computer systems). Therefore, money is accompanied with the knowledge about the ownership of namely this specific wealth. In operations with money, old knowledge changes to new knowledge.

The financial sector in Estonia (which is equivalent to the blood circulation in the human body) is almost fully computerized. The following facts are a good illustration of this claim:

- 98% of all bank transactions are completed via electronic means (on-line payments, credit card use, signing up for new bank services on-line etc). [6]
- 88% of all income tax declarations were entered on-line in 2008 and 17% of those on the first day of the declaration period. In 2009, the number of first day declarations rose 43%. [7]

The exchange of information is also largely facilitated by computer systems:

- major newspapers are represented on-line
- some key information forums are only available on-line
- medical records available to doctors via a national information system
- school grades, homework assignments and messages to and from parents are implemented in an e-school system
- Estonian police and courts use an e-case system, which allows for easy sharing of information about criminals

Leadership and management of the society is strongly reliant on computer systems:

- government holds paperless e-cabinet meetings
- local and state elections offer both manual and an electronic vote option

NB! This is not merely using „electronic gadgets“ but information transmitting, processing, storing etc. with computers in order to ensure the running of critical processes at the national level! Therefore, many (if not all) of these services should be considered critical information infrastructure and any attacks against them should be viewed in the context of national security. In most cases, attacks against these systems have a tangible effect on ordinary citizens, who can no longer get access to the services they need. This illustrates the dangers of over-dependence between human society and computer networks.

4 An Overview of the 2007 Spring Cyber Attacks Against Estonia

In the spring of 2007 many Estonian government and private information systems came under a wide scale cyber attack campaign that lasted for 22 days, from April 27th to May 18th. The attacks were a response to the Estonian Government's decision to relocate a Soviet WWII monument to a military cemetery. The decision met with much criticism by the Russian authorities, as well as the ethnic Russian minority in Estonia. Following two nights of looting and rioting in Tallinn, a campaign of cyber attacks was launched by presumably ethnic Russian activists, located in Russia, Estonia and elsewhere. To this day no official connection has been made to the Russian government. [8]

Majority of the attacks were relatively simple and robust, using well known methods and vectors. Most prominent were the distributed denial of service attacks (SYN flood, PING flood, mass e-mail etc.) which were launched both manually and via

botnets. However, the size and length of the attack was unexpected for most targets and therefore various services were either degraded or disabled throughout the conflict. The most prominent target categories were: government web and e-mail servers, on-line banking services, on-line news services, as well as the network infrastructure (DNS servers and network routers) at ISP level. [8]

It is important to note that this was a purely political attack – there is no information about financial motivation among the attackers. And yet, many "civilian" systems were purposefully targeted, including commercial banks and private news companies. This would indicate that the attackers were interested in damaging the Estonian cyber society in all the relevant categories identified in the introduction:

- targeting the banking infrastructure has serious economic consequences if services remain out of operation for more than a few hours or days
- attacks against news services bring about an (partial) information blockade both nationally and internationally (fortunately alternative media channels were not affected by this attack)
- attacks against government systems diminish the government's ability to properly govern the state.

In this light, the attackers were aiming at critical sectors of the Estonian cyber society, but were fortunately unable to cause serious harm. However, attacks like this are becoming more commonplace and should be addressed at a national level for any country that is in the process of transforming into a cyber society.

5 On Cooperation

An important lesson from these attacks is that the Internet has empowered the people not only by giving them access to information and nearly free communication around the globe, but also by letting people attack any connected target no matter the physical location. While this is usually not a problem, it can become one quickly enough if a critical mass of attackers converges on a target. Simplest denial of service attacks require no training or specialized software, so it is just a matter of finding enough committed attackers and coordinating their effort.

As a result of this relative ease we witness cyber attacks becoming more popular as a tool for political activism. Politically motivated cyber attacks have become commonplace. It is no longer surprising if a military conflict in Israel coincides with hacking on both sides, or if a political row between Russia and its neighbors also escalates into cyber space. In essence, cyber militias are developing in many countries around the world, some of them undoubtedly with the (passive?) support of the interested government. [9]

Since these cyber conflicts lack a clear legal status they usually boil down to technical countermeasures at the service provider and target level. Usually the attacks cross international boundaries, which means that the service providers and incident handlers (computer emergency response teams) need international cooperation in order to stem the tide of the attacks.

6 The Cooperative Cyber Defence Centre of Excellence

Understanding the importance of cooperation in cyber defence, in 2004 Estonia offered to establish and host a multi-national organization focused on developing this aspect within NATO. The Alliance supported this idea and after thorough preparation the Cooperative Cyber Defence Centre of Excellence (CCD COE) was formally established in the spring of 2008 and accredited as an International Military Organization in the fall of 2008. In addition to Estonia, it currently includes six more sponsoring nations: Germany, Italy, Latvia, Lithuania, Slovak Republic and Spain, with a few more in the process of joining the Centre.

The nature of the CCD COE is to develop new concepts, methods, tools, training materials, as well as analytical products. It is by no means intended or equipped as an operations organization, such as the various computer incident response teams etc. Instead, it is designed as a vessel for assisting NATO's transformation process, especially in the matters of cyber defence.

Organizationally the CCD COE is divided into three branches: administrative, research and development, training and doctrine. However, much of the work is done using a virtual matrix structure that "ignores" the official organization chart and uses the necessary manpower as ad-hoc project teams, regardless of the position of the personnel. This allows for a much more flexible approach when tackling complex problems.

7 Summary

As information technology becomes ever more integrated into our daily life, we transform into a cyber society. We have discussed that cyber society is, in fact, an advanced form of human-computer interaction, which encompasses the relationship between a society of humans and a network of computers.

In the preceding sections we have briefly covered the definition of information that is based on the concept of knowledge and main principles to corrupting it. We defined the concept of cyber society, identified Estonia as an early cyber society and examined the cyber attacks that brought this into focus in 2007. Finally, we discussed the principles behind the establishment and running the Cooperative Cyber Defence Centre of Excellence.

References

1. Wiener, N.: The human use of human beings. Cybernetics and society. Doubleday Anchor Books, Doubleday&Company, Inc., Garden City, New York (1956)
2. Fraenkel, A.A., Bar-Hillel, Y.: Foundations of Set Theory. North-Holland Publishing Company, Amsterdam (1958)
3. Potter, M.: Set Theory and its Philosophy. Oxford University Press, Inc., New York (2004)
4. Lorents, P.: Formalization of data and knowledge based on the fundamental notation-denotation relation. In: Proceedings of the International Conference on Artificial Intelligence, IC-AI 2001, Las Vegas, USA. USA, vol. III, pp. 1297–1301. CSREA Press (2001)

5. Lorents, P.: Knowledge and Taxonomy of Intellect. In: Proceedings of the International Conference on Artificial Intelligence, IC-AI 2008, Las Vegas, USA, July 25-28, vol. II, pp. 484–489. CSREA Press (2008)
6. Hiie, I.: Sulgkerged teenuste halduse protsessid. In: ITSMF 2007 conference, Tallinn, Estonia, November 22 (2007), http://www.itsmf.ee/itsmf2007/itsmf_estonia_2007_sulgkerged_protsessid.pdf (last accessed March 16, 2009)
7. Estonian Tax and Customs Board: Press Release (February 16, 2009), http://www.emta.ee/?id=25369&tpl=1026 (last accessed March 15, 2009)
8. Ottis, R.: 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, Plymouth, UK, June 30-July 1, pp. 163–168. Academic Publishing Limited, Reading (2008)
9. Ottis, R.: Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability. In: Proceedings of the 8th European Conference on Information Warfare and Security, Lisbon, Portugal, July 6-7, 2009 (accepted for publication)

VI Ottis, R. (2009) Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability. In *Proceedings of the 8th European Conference on Information Warfare and Security, Lisbon*. Reading: Academic Publishing Limited, p 177-182.

Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability

Rain Ottis
Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia
rain.ottis@ccdcoe.org

Abstract: Recent events in Estonia and Georgia have elevated the threat of cyber attacks to the international consciousness. While this has added visibility to the topic, it has not brought more clarity to the discussion. Terms like cyber warfare and cyber terrorism are widely used, but their definitions are rarely agreed upon. As a result, there is lot of skepticism about the true nature of cyber threats and whether governments are engaging in such attacks in cyberspace. It should be safe to assume that all governments are developing and using defensive cyber capabilities to some degree. Defending computer systems is considered a right and typically legal frameworks support such activity. As soon as one goes on the cyber offensive, however, they are off the map. There is little consensus, let alone legal guidance, regarding the use of cyber attacks to further a political or military goal. Very few nations have announced an offensive capability in cyber space, but it is reasonable to assume that more are covertly creating such a capability. In this paper the term offensive cyber capability is used instead of the better known computer network attack (CNA). Offensive cyber capability differs from CNA by including actors from outside the direct control of the government, such as freelance hackers, criminals and flash mobs as possible extensions to a nation-state's offensive capability. This paper offers a theoretical model composed of three approaches that a nation-state might use when creating an offensive cyber capability. First, the traditional use of 'own forces' is analyzed. The second way is to cultivate a volunteer force that can be guided to attack designated targets with little or no attribution to the government. The last approach is to outsource the problem to digital mercenaries. Each option has unique benefits and drawbacks, while some aspects remain universal across the board. In reality, the most effective approach is most likely a combination of all three.

Keywords: Offensive cyber capability, cyber attack, computer network attack, People's War

1. Introduction

Attacks in cyberspace have been a part of many international conflicts over the last ten years (Geers 2008). Arguably the most influential of these attacks occurred in Estonia in 2007 and in Georgia in 2008. It is notable, however, that in both cases the attackers remained largely anonymous and no direct state sponsorship has been proven in either cyber campaign. Instead, it looks like the attacks were planned and launched by concerned individuals who merely were expressing their political views via computer hacking. While this approach may be true on the surface, it fails to explain the lack of international law enforcement cooperation and open propaganda support for the attackers by the Russian authorities (Ottis 2008, Carr 2008).

This paper proposes a theoretical model that consists of three general ways to create a nation-state level capability to inflict damage on another nation-state or even non-state actors via cyber attack. The first option is the 'do-it-yourself' approach, or using the nation-state's own forces. The second is to cultivate a volunteer force that can be guided to attack designated targets with little or no attribution to the government. The last approach is to outsource (parts of) the problem to other governments, commercial entities or the criminal underworld in a mercenary model. As shown in Figure 1, combinations of two or three approaches can also be used, if there a need for it exists. The benefits, drawbacks and ways to recognize each approach are qualitatively analyzed in the following chapters.

According to Joint Publication 3-13 (Information Operations), computer network operations (CNO) represent one of the five core capabilities of information operations (IO). CNO, in turn, consists of three elements: computer network attack (CNA – offensive), computer network defense (CND – defensive) and computer network exploitation (CNE – intelligence). In this paper the term *offensive cyber capability* is used instead of the better known CNA, which refers to "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves" (JP 3-13 2006). The difference between CNA and offensive cyber capability is not in the action, but with the actor. While not explicitly stated as such, the implied actor of a government-backed computer network attack in the context of information operations seems to be an organic part of the government (for example, a military unit). Offensive cyber capability, however, includes actors outside the direct control of the government. For example, freelance hackers, criminals and flash mobs can be used to attack a target by proxy, thus extending the offensive cyber capabilities of a nation-state.

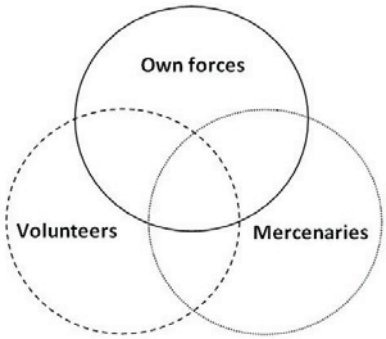

Figure 1: Three approaches for setting up an offensive cyber capability

2. The "own forces" approach

Historically, if a new capability is required by a state, it is often done with redistributing existing resources in the state apparatus or by creating a new body to take on the task. It is a natural approach for a government and it ensures that the activities are under the government's control. Need to put an American into orbit? No problem, let there be NASA. Need to project your military power in cyberspace? No problem, let there be a Cyber Command to plan, prepare, execute and exploit cyber attacks as part of everyday military activity.

The Cyber Command mentioned above is just an abstract example – a cyber force could take many forms from straightforward regular military units to shadowy intelligence agencies to scientific red teams. The common factors they all share are professional membership and a clear and unambiguous link to the state. The state link enables cooperation and coordination with national military/intelligence/law enforcement, although this is very likely seldom achieved in full. However, even partial coordination with physical operators will surely multiply the effect of a cyber attack and *vice versa*. For example, an air strike against an enemy radar system would be much more effective if cyber attacks could disable the missile batteries guarding the site.

Setting up another unit or agency for this purpose should be a routine process and most likely easily accommodated by the legal framework of the state. The main question may be the policy issue of creating an *offensively* oriented organization but there are solutions for that as well. The simplest option could be to create this organization in secret and add it to the intelligence structure.

A different aspect of maintaining a low profile is the fact that some of the cyber attacks can fall outside the current box of legal tools and toys. Arguably this question may not emerge in a straightforward military conflict where tanks, helicopters and ships are used to deliver more tangible damage every day. A cyber attack could be categorized as just another activity to gain a military advantage over the enemy. The problem is that much of the military infrastructure is linked to, if not based upon, civilian infrastructure. Therefore, a cyber attack against a military target may cause considerable collateral damage. To make matters even worse, civilian systems (banks, internet service providers, phone companies etc.) may become primary targets in a conflict as they will hamper the economy of the target nation (war of attrition) or disrupt the target nation's ability to communicate with the outside world (communications jamming or information blockade). Therefore, the layer of secrecy may be required in order to protect the cyber warriors from potential legal consequences.

States tend to be fairly secretive about the specifics of their defense budget. As a result, a significant amount of resources can be channeled to build up an offensive cyber capability to the required level without much fuss in the public eye. Therefore, the absence of a published doctrine does not always mean a lack of capability or intent. If it is in the state's interest to keep the creation of an offensive cyber unit a secret, they are well within their rights to do so.

One of the main benefits of having a state-run organization is direct access to the state's resources and the ability to coordinate actions within a unified framework. Access to state funds, personnel and training resources can provide a strong, disciplined, well-equipped and trained force that is on call at a moment's notice. Thus the key strengths of this approach are reliability, predictability and control.

However, this approach does have its weaknesses. Of the three options considered here, it is likely the most expensive one to implement. Having a pool of trained experts on call takes a lot of resources, considering that they may never see any action. This problem is similar to the one haunting nuclear forces.

The second problem relates to attack attribution. In a pure military style cyber attack against a specific target, it is very difficult to deny state involvement, even if the trail goes cold in a third party country. The methodical approach that a government run operation would likely take could also indicate who the attacker is. Furthermore, creating a cyber storm to provide the necessary background noise would most likely affect some collateral targets. This would invoke a host of potentially troublesome legal issues. For example, consider having to explain to the international community why it was necessary to attack a multi-national bank in order to apply political or military pressure on an adversary government. In fact, it is possible that similar line of reasoning has deterred at least one potential state level cyber attack against a civilian target in the past. During the Kosovo campaign the US forces supposedly considered hacking Milosevic's foreign bank accounts but were not given a green light to execute (Yurcik 2001).

In order to identify a cyber attack sponsored by a nation-state, an observer should be looking for the following signs:

- the state in question may have an official policy and designated organization(s) for carrying out offensive cyber operations;
- a state's traditional military operations could 'coincide' with cyber attacks;
- the political enemies of the state (internal and/or external) may be targeted by cyber attacks that do not display typical criminal motivation (money), especially when politically-favored organizations suffer few or no attacks;
- law enforcement does not make any effort or progress in catching attackers suspected of living within their borders.

3. Volunteer force approach

The wide-scale adoption of information technology has undoubtedly transformed both government and civil society over the past two decades. One aspect of this transformation is that people now have unprecedented access to information and global communications. The Internet is an ideal tool for sharing ideas, finding contacts, and creating new business opportunities. In that sense, the Internet has empowered people. On the other hand, it also means that people are now empowered to carry out new types of attacks against other residents of the information society.

While the original, stereotypical hacker may have been a lonely specialist looking for an intellectual challenge, many cyber attacks today are carried out by criminals or political activists. When criminals conduct cyber attacks for financial gain, political activists participate in such campaigns to support a particular ideology. It is this politically active and potentially dangerous segment that can be harnessed as a volunteer cyber militia. As recent political cyber campaigns in Estonia, Georgia, and Israel show, individuals can and will take part in cyber attacks against state targets. The question is whether this force can be mobilized in a timely and controlled manner.

It is important to note, however, that most volunteer cyber militias have a spontaneous start, likely based on an underlying grass roots movement or community. It is not known, how many and if some of these have been set up by deliberate government action. Nevertheless, it is possible for a government to 'hijack' a cyber militia by either infiltrating its ranks or applying pressure on the membership.

Managing a volunteer cyber force could be achieved in many ways. For example, by persuading existing 'hacker' organizations to work for the state or by setting up a new organization to run a proxy campaign for the government. Alternatively, the state may indirectly *guide* the citizens or supporters to take part in cyber attacks individually, without actually relying on any real, underlying organization.

Such a loose network of attackers could be very difficult to defend against, because the different skill sets, locations, time zones and resources of the attackers could make the attack large in volume as well as highly heterogeneous in nature. There would be no 'silver bullet' defense that could effectively

cut off all the attackers, aside from cutting the target's connection to the outside world altogether. Volunteers representing large nations (and their diaspora) or global political movements are well placed to carry out around-the-clock attacks for extended periods of time. Further, if some attackers are identified, their arrest will have little direct impact on the rest of the attackers. The only noteworthy effect would likely be psychological, but this could either discourage other attackers or it could recruit more fighters to the cause.

An added bonus for using a volunteer force is that the state could deny any links to cyber attacks, as they would seem to come from individuals with no direct link to the state. This is true only if the state can manage the volunteers in an indirect manner. One way is to infiltrate the volunteer community with provocateur and motivator agents who use propaganda and other psychological operations techniques to manipulate the volunteers. This would not be very difficult, because the volunteer community typically communicates and 'meets' via online forums, discussion groups, etc. Authentication, if attempted or desired, is very difficult to enforce and can be circumvented with 'sleeper' agents.

This type of indirect control brings out one of the chief weaknesses of this approach: unpredictability. It is impossible to accurately predict what the reaction of the community will be to orders from the state. How fast will they mobilize? What skills and resources will they contribute? Will they attack collateral targets and needlessly expand the conflict? When will they finish - too soon or too late? These questions remain unanswered and they illustrate the potential dangers that are inherent in this approach. Therefore, planning a "People's War" campaign (Wu 2004) would have to incorporate a wide margin for error. As a precursor to a conventional military attack or as a digital harassment campaign, this may not matter, as the main goal of the cyber attack could be simply to confuse the target.

An interesting aspect of the volunteer force approach is that offensive campaigns would have to be relatively frequent and regular. In essence, one would have to make sure that the 'reserve' is trained and ready to fight. The only way to do this is to make sure they have a 'training exercise' every now and then, because otherwise they may find something better to do. This concept of *training the reserve* has several negative side effects: increase in related cyber crime, tense relations with political opponents (national or international) and the potential for the force to be overextended. If the attack campaigns occur too frequently or are used against strong opponents, then the motivation level of the volunteers will likely drop and they may find an alternative pastime.

On a positive note, compared to the other options presented here, a volunteer force is likely the cheapest version in terms of direct costs. The time, resources and training of the volunteers will be covered by the volunteers themselves. The only real direct costs to the state are to hire some agents to spur and direct the volunteers. The indirect costs from rising cyber crime levels and lost productivity, however, may significantly decrease the economic effectiveness of this option.

It is important to note that by using an indirectly-controlled volunteer approach, the state would have to cultivate a society where cyber attacks are an acceptable course of action. Political attacks like this can't be prosecuted by law enforcement, as this would discourage people from volunteering. On the other hand, accepting cyber attacks as a valid political tool may provoke an undesired cyber campaign against the sponsoring government in the future.

To identify the managed volunteer approach, an observer should be looking for the following signs:

- the state publicly glorifies people who have participated in cyber attacks against the state's 'enemies';
- the political enemies of the state (internal and/or external) are often targeted by cyber attacks that do not display typical criminal motivation (money), while politically-favored organizations suffer few or no attacks;
- law enforcement does not make any effort or progress in catching the attackers.

4. Mercenary approach

While outsourcing may be a widely accepted business practice, it is rarely an acceptable solution for an organization's core business functions. The same holds true for national security and military power. Transporting fuel to the operations area may be left to civilian freight companies, whereas

engaging with the enemy should be done by one's regular armed forces. As such, the possibility of outsourcing the *offensive cyber capability* of a state may not come naturally for a government. However, this does not mean that it can't be done.

Employing mercenaries is possible, but often not a scalable solution. Conducting raids and providing personal security is one thing, but the cost of running a mercenary *army* to fight an all-out war would probably be too high for most, if not all, states. However, two aspects make this option different in a cyber conflict. First, a cyber attack need not be very wide spread in order to seriously hurt the target. Second, cyber attacks are asymmetric in nature, where the number of attackers can be less important than in the physical world. Skill, time and knowledge of the target infrastructure can more than make up for any deficiencies in numbers. Therefore, outsourcing the cyber attack to a group of digital mercenaries is a viable option from a financial perspective. Indeed, it is probably much cheaper than to organize, train and maintain a conventional unit that is only rarely needed.

Practical examples of outsourcing cyber attacks include renting a botnet for denial of service attacks, contracting hackers to take down a specific website, or asking an ally to help out. As the last example indicates, not all the options here need to be illegal.

Outsourcing the capability is very useful if the intent is to conduct a non-attributable campaign. If the state does not have an official policy, organizational structure or the know-how to conduct an offensive cyber campaign, then it is very hard to prove that the state is behind the attacks that were launched by well-known criminal organizations.

Obviously the outsourcing option also has drawbacks. The biggest is most likely reliability, as it is very difficult to guarantee that the service is available when needed and meets the required level of quality. Another worry is a loss in international prestige if the link ever comes out. Another logical threat is that the outsourcing party may at some point change sides or go rogue and start to blackmail the government.

If criminals are used then a very important secondary effect could come back to haunt the state. In order to maintain a working relationship with them, the state must in effect allow them to pursue their criminal activities. It is very unlikely that a criminal organization will provide a service to the government if its members are being hunted down and prosecuted for everyday crime. Therefore, the crime level, especially cyber crime, will likely increase in the country that has chosen the outsourcing option. However, this kind or approach requires a moral ambiguity from the government to begin with and it follows that the government may not consider these effects a problem.

Obviously, it is possible to contract these services from a criminal organization in a different country as well, but then the state has much less control over the attacks and fewer levers to manipulate the criminals.

To discover a possible use of the mercenary outsourcing option, an observer should look for the following signs:

- cyber criminals get very light sentences or are released early for unclear reasons;
- the political enemies of the state (internal and/or external) are often targeted by cyber attacks that do not display typical criminal motivation (money), while politically-favored organizations suffer few or no attacks;
- law enforcement does not make any effort or progress in catching attackers suspected of residing within their borders.

5. Comparison of the approaches

When comparing these three approaches to managing cyber attacks, it is clear that in reality a combination of two or three approaches might be used. For example, volunteer campaigns can raise funds to buy botnet time from the criminals.

The most important reason to adopt the 'own forces' approach is to have direct control over the attacking force. While outsourcing to mercenaries may provide some quality-of-service guarantees, it will never be on par with the control over integrated military units. Volunteers may or may not be

interested in the current conflict and they may also get out of control, expanding the conflict and potentially provoking a third party to enter on behalf of the adversary.

In terms of direct costs for setting up an offensive cyber capability for a state, the volunteer option is probably the cheapest, while the 'own forces' approach is the most expensive. The volunteer and mercenary options do incur a sizeable secondary cost in terms of higher crime levels and lost productivity. Therefore one shouldn't make decisions based on the up-front costs alone.

Depending on the goals and the moral stance of the state, it may be necessary to keep offensive cyber activities secret, no matter what approach is chosen. This is especially important if the state needs plausible deniability to distance itself from the attacks. The proper attribution of cyber attacks will always be a difficult task, but building in an extra layer of secrecy – as well as ensuring a lack of law enforcement cooperation – will make it a futile task.

6. Limitations and future work

This paper does not consider sub-state level actors acting on their own agenda. Nevertheless, the three approaches described here should be applicable to commercial entities, organizations and even private persons. The main interest, however, remains on the capabilities of nation-states, as they have the most resources and the strongest influence in the international political arena.

The approaches presented here provide just one way of analyzing this subject area. They are by no means meant to exclude any other frameworks or models and should be considered an effort to bring greater understanding to the still developing concept of cyber warfare.

Of the three approaches presented above, the volunteer option remains the most intriguing for further study. Every year brings more examples of this approach to light; whether they are spontaneous in nature or driven by covert government action is unknown. As such, there are many data points from which to build a theoretical framework for this approach. More specifically, the methods for organizing such a force and developing a method for estimating or measuring the potential effectiveness of a volunteer campaign will remain in focus for the coming year.

7. Conclusion

Understanding the nature of cyber warfare is a difficult task, but one that must be attempted nonetheless. While warfare has been typically a prerogative of a state, the various forms it can take often include non-state actors. Volunteer guerilla fighters and hired mercenaries have often turned the tide of battle, if not the war. Therefore, it is logical to assume that digital versions of non-state fighters will also have an important role to play in nation-state level cyber conflicts. Moreover, it may be in the interests of some states to harness this force and to integrate it into the state's overall offensive capabilities. The three approaches described in this paper form a theoretical model of the options available to a nation-state. Often, due to limited resources, it may be more useful for a state to cultivate a volunteer cyber militia instead of building a fully professional force. And volunteers, especially if they are free of restrictions (legal concerns, doctrinal constraints etc.), can be resourceful and flexible, thus achieving success where a conventional force may fail.

References

Carr, J. et al. (2008) *Russia/Georgia Cyber War – Findings and Analysis*. [Online] Project Grey Goose. Available at: http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report. [Last accessed 04 February 2009]

Geers, K. (2008) "Cyberspace and the Changing Nature of Warfare." In *NATO RTO Symposium on Information Assurance for Emerging and Future Military Systems*, Ljubljana.

Joint Publication 3-13. Information Operations. (2006) Chairman of the Joint Chiefs of Staff. Available at: http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf. [Last accessed: 05 February 2009]

Ottis, R. (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*. Reading: Academic Publishing Limited, pp 163-168.

Wu, C. (2004) "An Overview of the Research and Development of Information Warfare in China." In Edward Halpin et al (eds.) (2006) *Cyberwar, Netwar and the Revolution in Military Affairs*. Palgrave MacMillan, Hampshire, pp 173-195.

Yurcik, W. and Doss, D. (2001) "Internet Attacks: A Policy Framework for Rules of Engagement." [Online] In *The 29th Research Conference on Communication, Information and Internet Policy*, Alexandria. Available at: http://arxiv.org/ftp/cs/papers/0109/0109078.pdf. [Last accessed: 03 February 2009]

DISSERTATIONS DEFENDED AT TALLINN UNIVERSITY OF TECHNOLOGY ON *INFORMATICS AND SYSTEM ENGINEERING*

1. **Lea Elmik**. Informational modelling of a communication office. 1992.
2. **Kalle Tammemäe**. Control intensive digital system synthesis. 1997.
3. **Eerik Lossmann**. Complex signal classification algorithms, based on the third-order statistical models. 1999.
4. **Kaido Kikkas**. Using the Internet in rehabilitation of people with mobility impairments – case studies and views from Estonia. 1999.
5. **Nazmun Nahar**. Global electronic commerce process: business-to-business. 1999.
6. **Jevgeni Riipulk**. Microwave radiometry for medical applications. 2000.
7. **Alar Kuusik**. Compact smart home systems: design and verification of cost effective hardware solutions. 2001.
8. **Jaan Raik**. Hierarchical test generation for digital circuits represented by decision diagrams. 2001.
9. **Andri Riid**. Transparent fuzzy systems: model and control. 2002.
10. **Marina Brik**. Investigation and development of test generation methods for control part of digital systems. 2002.
11. **Raul Land**. Synchronous approximation and processing of sampled data signals. 2002.
12. **Ants Ronk**. An extended block-adaptive Fourier analyser for analysis and reproduction of periodic components of band-limited discrete-time signals. 2002.
13. **Toivo Paavle**. System level modeling of the phase locked loops: behavioral analysis and parameterization. 2003.
14. **Irina Astrova**. On integration of object-oriented applications with relational databases. 2003.
15. **Kuldar Taveter**. A multi-perspective methodology for agent-oriented business modelling and simulation. 2004.
16. **Taivo Kangilaski**. Eesti Energia käiduhaldussüsteem. 2004.
17. **Artur Jutman**. Selected issues of modeling, verification and testing of digital systems. 2004.

18. **Ander Tenno**. Simulation and estimation of electro-chemical processes in maintenance-free batteries with fixed electrolyte. 2004.

19. **Oleg Korolkov**. Formation of diffusion welded Al contacts to semiconductor silicon. 2004.

20. **Risto Vaarandi**. Tools and techniques for event log analysis. 2005.

21. **Marko Koort**. Transmitter power control in wireless communication systems. 2005.

22. **Raul Savimaa**. Modelling emergent behaviour of organizations. Time-aware, UML and agent based approach. 2005.

23. **Raido Kurel**. Investigation of electrical characteristics of SiC based complementary JBS structures. 2005.

24. **Rainer Taniloo**. Ökonoomsete negatiivse diferentsiaaltakistusega astmete ja elementide disainimine ja optimeerimine. 2005.

25. **Pauli Lallo.** Adaptive secure data transmission method for OSI level I. 2005.

26. **Deniss Kumlander**. Some practical algorithms to solve the maximum clique problem. 2005.

27. **Tarmo Veskioja**. Stable marriage problem and college admission. 2005.

28. **Elena Fomina**. Low power finite state machine synthesis. 2005.

29. **Eero Ivask**. Digital test in WEB-based environment 2006.

30. **Виктор Войтович**. Разработка технологий выращивания из жидкой фазы эпитаксиальных структур арсенида галлия с высоковольтным p-n переходом и изготовления диодов на их основе. 2006.

31. **Tanel Alumäe**. Methods for Estonian large vocabulary speech recognition. 2006.

32. **Erki Eessaar**. Relational and object-relational database management systems as platforms for managing softwareengineering artefacts. 2006.

33. **Rauno Gordon**. Modelling of cardiac dynamics and intracardiac bio-impedance. 2007.

34. **Madis Listak**. A task-oriented design of a biologically inspired underwater robot. 2007.

35. **Elmet Orasson**. Hybrid built-in self-test. Methods and tools for analysis and optimization of BIST. 2007.

36. **Eduard Petlenkov**. Neural networks based identification and control of nonlinear systems: ANARX model based approach. 2007.

37. **Toomas Kirt**. Concept formation in exploratory data analysis: case studies of linguistic and banking data. 2007.

38. **Juhan-Peep Ernits**. Two state space reduction techniques for explicit state model checking. 2007.

39. **Innar Liiv**. Pattern discovery using seriation and matrix reordering: A unified view, extensions and an application to inventory management. 2008.

40. **Andrei Pokatilov**. Development of national standard for voltage unit based on solid-state references. 2008.

41. **Karin Lindroos**. Mapping social structures by formal non-linear information processing methods: case studies of Estonian islands environments. 2008.

42. **Maksim Jenihhin**. Simulation-based hardware verification with high-level decision diagrams. 2008.

43. **Ando Saabas**. Logics for low-level code and proof-preserving program transformations. 2008.

44. **Ilja Tšahhirov**. Security protocols analysis in the computational model – dependency flow graphs-based approach. 2008.

45. **Toomas Ruuben**. Wideband digital beamforming in sonar systems. 2009.

46. **Sergei Devadze**. Fault Simulation of Digital Systems. 2009.

47. **Andrei Krivošei**. Model based method for adaptive decomposition of the thoracic bio-impedance variations into cardiac and respiratory components.

48. **Vineeth Govind**. DfT-based external test and diagnosis of mesh-like networks on chips. 2009.

49. **Andres Kull**. Model-based testing of reactive systems. 2009.

50. **Ants Torim**. Formal concepts in the theory of monotone systems. 2009.

51. **Erika Matsak**. Discovering logical constructs from Estonian children language. 2009.

52. **Paul Annus**. Multichannel bioimpedance spectroscopy: instrumentation methods and design principles. 2009.

53. **Maris Tõnso**. Computer algebra tools for modelling, analysis and synthesis for nonlinear control systems. 2010.

54. **Aivo Jürgenson**. Efficient semantics of parallel and serial models of attack trees. 2010.

55. **Erkki Joasoon**. The tactile feedback device for multi-touch user interfaces. 2010.

56. **Jürgo-Sören Preden**. Enhancing situation – awareness cognition and reasoning of ad-hoc network agents. 2010.

57. **Pav**el **Grigorenko**. Higher-Order Attribute Semantics of Flat Languages. 2010.

58. **Anna Rannaste**. Hierarcical Test Pattern Generation and Untestability Identification Techniques for Synchronous Sequential Circuits. 2010.

59. **Sergei Strik**. Battery Charging and Full-Featured Battery Charger Integrated Circuit for Portable Applications. 2011.