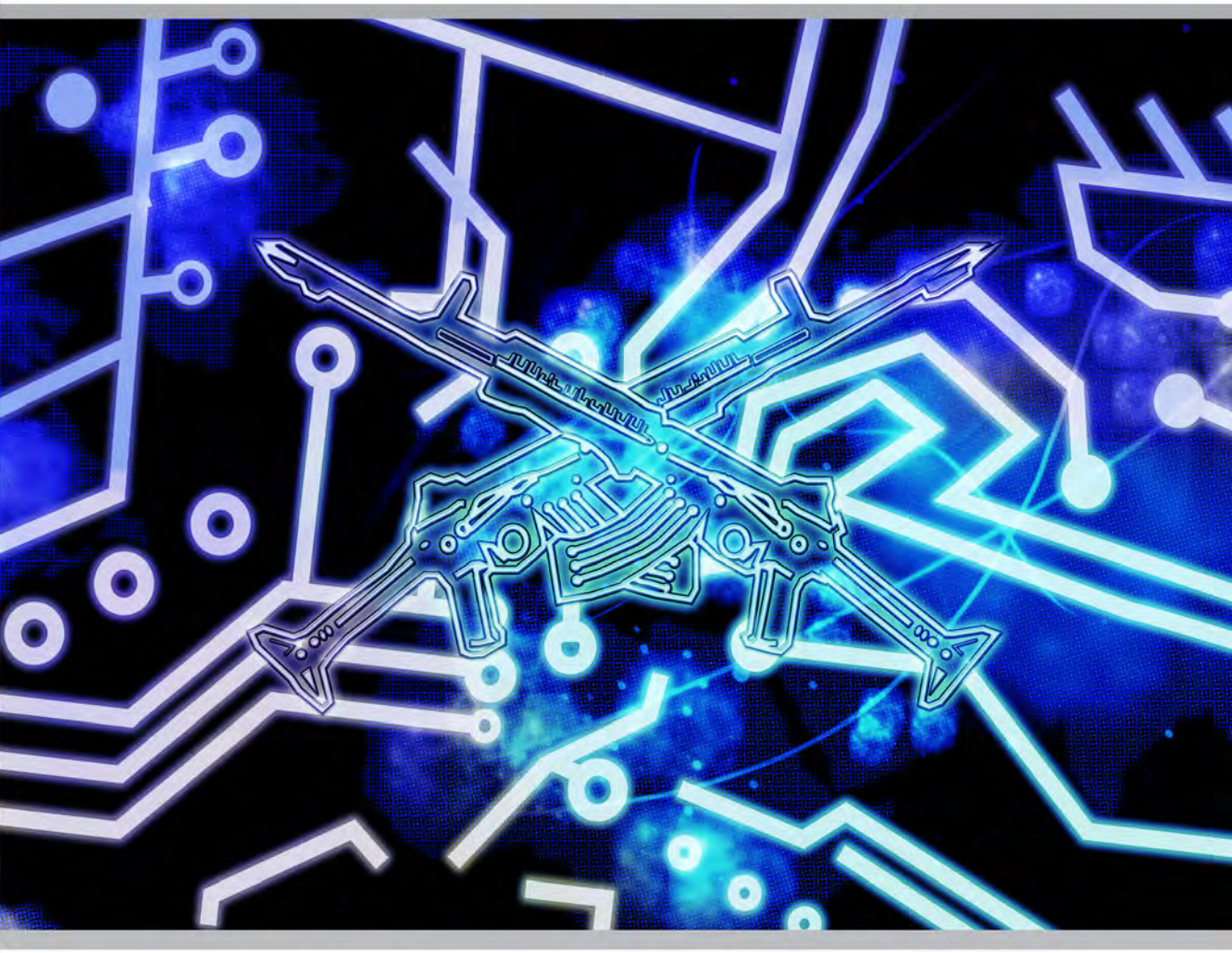
THE FOG OF CYBER DEFENCE



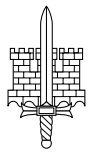
Jari Rantapelkonen & Mirva Salminen (eds.)

National Defence University
Department of Leadership and Military Pedagogy

Series 2: Article Collection N:o 10

THE FOG OF CYBER DEFENCE

Eds. Jari Rantapelkonen & Mirva Salminen



National Defence University
Department of Leadership and Military Pedagogy
Publication Series 2
Article Collection n:o 10
Helsinki 2013

ISBN 978–951–25–2430–3
ISBN 978–951–25–2431–0 (PDF)
ISSN 1798–0402

Cover: Toni Tilsala/National Defence University
Layout: Heidi Paananen/National Defence University

Juvenes Print Oy
Tampere
2013

CONTENTS

Foreword

Internet is a good example of how technology can dramatically alter our everyday lives. In the past two decades, Internet has evolved from the "playground of the geeks" to a serious tool to do business with. With a single click of a mouse, it is possible to share information with millions of people. Unfortunately, this evolution has also brought about all of the negative side effects of global communication and digital freedom. As the tip of the iceberg, Internet is full of junk mail, malware, scam, and identity thefts – just to name a few examples. Simultaneously, we – the benevolent users – are suffering more and more from attacks on the availability of services and information.

Similarly like the mobile phones, Internet has become a commodity without which our modern lifestyle would not survive. Therefore, we have seen governmental level strategies to "protect our critical information infrastructures" or to "secure cyberspace". Neither Internet, nor any other communication channel is anymore controllable by a single entity, government or corporate. On the contrary, they are networks of networks on which we have very little control on how they evolve.

We are living in a world of ubiquitous computing, where various computing devices are communicating and sharing information around us, for us, and about us. Clouds of computers are formed and deformed dynamically without any need of human intervention. World Wireless Research Forum, WWRF, has predicted that there will be seven billion mobile phones in the world by the year 2017. At the same time, the number of computers will rise to seven trillion, that is, there will be roughly a thousand computing devices per person. Thus, our physical space and "cyberspace" will overlap completely.

When considering cyberspace from the military perspective, we can ask whether cyber will cause an evolution or a revolution in warfighting. On the one hand, cyber enables us to "see, hear, and talk" faster and over longer distances, which enables us to perform our military objectives faster and with a greater accuracy. On the other hand, cyber is a totally different battlefield with different rules and engaged players than the conventional land, sea, air, and space.

This book generates new ideas and opens new topics of discussion with regard to cyber. Even though bits usually do not kill – at least, not directly – we must consider the consequences of cyber operations also from the military perspective. Plenty of questions will rise on this research area, such as "Who are the enemies?"; "What are the rules of engagement?"; "Shall we be defensive or offensive in Cyber?"; and "How do we define 'credible defence' in cyber?".

Hannu H. Kari
Research Director, Professor, National Defence University

SUMMARY

The Fog of Cyber Defence is a study made primarily for the NORDEFCO (Nordic Defence Cooperation) community. Nonetheless, it can be applied to other contexts in which enhanced understanding of the challenges of cyberspace is important. The research project was originally called *Cyber Defence in the Nordic Countries and Challenges of Cyber Security*. For the purposes of the book and due to issues that were raised during the project, the name was changed to better describe the significance and omnipresence of cyber in information societies. However, cyber remains very much a "foggy" challenge for the Nordic countries which are considered cyber savvies.

The book focuses on Nordic cooperation in the field of defence policy on a political level. It is a collection of articles that aim to answer the many questions related to cyber security and take a stand on the practical possibilities of cyber defence. The meeting of the Defence Ministers on the 12th and 13th of May 2009 was an example of political positioning with regard to cyber. All Nordic countries – Finland, Sweden, Norway, Denmark and Iceland – participated. In addition to familiar topics such as cooperation in crisis management, material cooperation and operational cooperation, the meeting also witnessed a new common will to deal with new challenges. In the same year, during the June 2009 meeting of the Ministers for Foreign Affairs in Reykjavik, the Nordic countries acknowledged the need for enhanced cooperation to respond more effectively to cyber security problems. Two years later, when the Foreign Ministers of Denmark, Finland, Iceland, Norway and Sweden met on the 5th of April 2011 in Helsinki, the ministers stated that the Nordic Declaration on Solidarity would be followed up with practical measures, such as cooperation in the field of cyber security. On the political level, there is a desire to move towards concrete and practical cyber cooperation. This study on cyber defence was assigned in the 2012 NORDEFCO MCC Action Plan, and it was Finland's turn to conduct a study of an area of interest that would be implemented within the NORDEFCO framework.

It was agreed that the recently commenced study, "Cyber Defence in the Nordic Countries and Challenges of Cyber Security," would form the basis for further exploration of possibilities for Nordic cooperation in the field of cyber defence.

Key Results

The concepts of cyber, cyberspace, cyber security and cyberwar are multidimensional and ambiguous. The key results support the development of a common language and understanding in cyber activities among the Nordic countries, as well as the development of practical cooperation. The phenomenon is greater than what a single country can deal with alone.

a) Cyberspace
   - The Nordic countries are the most developed countries in cyberspace. Simultaneously, they recognise the importance of and their dependence on cyberspace for managing the welfare and security of the countries and their citizens.

- Cyberspace is a vague domain in relation to state and defence activities. It raises many unanswered and significant philosophical, but also clearly critical national security questions about how states should relate themselves to cyberspace.
- Cyberspace has different qualities and attributes than physical spaces. Cyberspace can be described as a "ubiquitous," "networked", and "virtual" world, and cyber activities have even been considered "anonymous." If this is understood through power politics, bureaucracy and hierarchical leadership, new kinds of political practices can be created and cyber cooperation can be strengthened. In any case, cyberspace on its own forces the Nordic countries to continue modernising themselves.
- Activity in cyberspace is controlled by individuals and companies, and it is not state-centric. Despite the attempts, international organizations (such as the ITU and the EU) and states have at least not until now had a significant role in controlling the activity. We are prompted to ask whether states should give up the idea of control and adapt to cyberspace with a different kind of philosophy, objectives, and cooperation models than to which they are accustomed.
- The military has recognised cyberspace as an operational domain similar to land, sea, air and space, that is, as a space to be used for military purposes and for waging war.
- Social media makes events and issues more transparent. Transparency is a trend that is already present but not necessarily understood by the nation states and the armed forces.
- Cyberspace is still a new and ever-developing domain, which is evident, for example, in the lack of development in legislation.

b) Cyber Security
   - The Nordic countries use traditional security language to address a new security phenomenon, that is, the phenomenon of cyber security.
   - Problems relating to cyber security reach across the borders and resources of individual countries and thus, they cannot be resolved by a country alone.
   - Threats relating to cyber security are complex and do not involve only technology. They are mainly social and human, and implicate the diverse customs of different countries, organisations, companies and individuals. Cyber threats cannot be treated as isolated phenomena. Instead, they must be addressed jointly with other threats in which the cyber domain plays a significant role as an enabler. For this reason it is suggested that the multiple problems relating to cyber security should be resolved together.
   - Social media makes evident how widespread the challenge of cyber security actually is.
   - Cyber security is only in part a military challenge. It is mostly a challenge in other areas such as the technological, social, procedural, legislative, etcetera. The defence forces are not responsible for protecting countries from cyber threats in the Nordic countries.
   - State related threats (espionage, intelligence, offensive) are on the rise, and they are believed to be more serious than individual, group or network based threats. However, threats are relative and a state related threat towards a country is not necessarily a threat towards another country. In the Nordic countries, threats are

primarily seen as relating to the functionality of the society rather than directed expressly towards the state.

- All Nordic countries have cyber security strategies to address the challenges of cyberspace, but they differ in how they allocate resources and organise security activities.
- There is still an obvious need to raise cyber security awareness and to clarify the related roles and responsibilities on the governmental level. There is also an important need for enhanced cyber competence amongst decision makers.
- The Nordic countries lack significant cooperation in cyber security on a practical level.
- Concepts related to cyber security are important in defining the phenomenon. To overcome problems with the current concepts, such as offensive cyber defence and cyberwar, it is necessary to study new concepts, such as resilience or cyber resilience, which can reveal new perspectives for dealing with cyber threats and security.

c) Cyberwar

- The military is planning and preparing for cyberwar.
- There is no single cyberwar or a single type of cyberwar – like there is not only one type of land or air war. On the other hand, the whole concept of cyberwar as "real" war has been both promoted and questioned. However, war without any kind of use of cyber means seems now unlikely.
- Cyberwarfare is a hybrid that originates from heterogeneous sources; consists of different elements; produces the interaction of distinct cultures and traditions, as well as of different people and organisations.
- In future wars, the Nordic countries will be increasingly dependent on computers, electricity, electronics and networks. Therefore, it is difficult to imagine future wars without cyber activities.
- Several states and networks, rather than individual hackers, are developing cyber capabilities for attack. Destructive cyber attacks, such as Stuxnet, will increase in 2013 as states continue to develop offensive capabilities.
- Cyber weapons are very dynamic. The leading countries in cyberwarfare produce modular cyber weapons software with continuous updates, shared components and parallel independent lines of development.
- In practice, cyberwarfare capabilities are kept secret either for maintaining a deterrent, concealment and increasing competitive edge or due to the lack of offensive resources.
- There are businesses that weaponize and exploit codes to attack vulnerabilities in operating systems and applications. Vulnerabilities and codes have become the everyday trading goods of the cyber arms industry. On the other hand, there is a commercial effort to make exploited code worthless to the vendor. However, the real world in cyberwar is not black and white. Cyberwar and cyber security are weird and chaotic phenomena taking place in cyberspace.
- The best way to protect against cyberwar is the development of C4 systems to secure all processes and applications in use. However, the human nature and unpredictable behaviour remain the most important threats in future cyberwarfare. This idea seems to be counter to the current technological and procedural trends that the Nordic countries are heading towards in cyberspace, although, for example, cloud

services providing valuable information can be compromised if they are used in critical situations. The “do-it-alone era” has passed, regardless of this being the best approach in the past. Cyber security is full of compromises.

- Even computer programs and integrated chips are important in cyberwar. Human knowledge and understanding together with technology form the heart of cyberwar. Cyberwar is human, not just high-tech driven.
- Building cyberwar capabilities is politically sensitive. However, the related discourse has neglected this on the strategic level. A (political) country can be defensive, but on the operational (practical) level it should not limit its offensive capabilities. This also guarantees the effectiveness of strategic defence.
- The term “cyberwar” and its use need to be reconsidered: is cyberwar war at all? Regardless of the answer, different war-like phenomena take place in cyberspace and they have the potential to change warfare.

d) The Nordic Countries, Further Points

- **Finland** aims to be a globally strong player in the field of cyber and cyber defence. Originally known as information security, cyber defence has become an issue on the strategic and individual levels. Protection against threats requires strategic level decisions, because cyber defence not only depends on security technologies but also on strategic guidance and coordination, as well as on the allocation of resources. Cyber development has been rapid and currently Finland is struggling to keep her global leading position in this field. The current challenge is to decide how cyber security and cyber defence will be implemented in practice. Finland is known to have good cooperation between cyber actors within the country. However, in order for her to be successful in this area, she needs real practical decisions and new resources for cyber, national cooperation, as well as cooperation with globally leading countries.
- **Norway** released a revised "National Strategy for Information Security" in late 2012. This strategy is but the latest in a series of strategic documents on cyber security dating back to 2003. Norway has a long history of extensive cooperation in cyberspace, partly due to the nature of digital threats, but also a long history of civil-military cooperation in all areas relevant to crisis management (the concept of "Total Defence"). Norway defines threats against information and communication systems as a strategic security challenge, and the effort to protect against these threats is given a high priority. The endeavour to enhance Norway's cyber security is making progress in all sectors of society. The Norwegian national CERT has been provided increased funding for 2013, and the Norwegian Armed Forces Cyber Defence (NOR CYDEF) changed its name in the second half of 2012 in order to underscore the increased importance of cyber defence in the military sector.
- **Sweden** Swedish cyber defence aims at protecting Sweden and the Swedish interests against cyber attacks from resourceful and advanced players. This includes strategic control and planning, cooperation and coordination as well as operational protection measures. Sweden is looking to the future and developing cyber fields such as automated information collection, sensor information and analysis of events. She is focused on creating robust information infrastructures and effective technical and administrative security processing. Cooperation and exchange of information are becoming increasingly important. Authorities are setting up routines for incident

reporting and information sharing between the different CERTs, to other authorities, to the private industry and to international organisations. Coordination, exercises and exchange of information with skilled and well-informed parties internationally is a top priority for the Swedish Armed Forces, as well as for other authorities that are in charge of national cyber security. Future options and scenarios are still open, but the idea is that the future Swedish Computer Network Operations (CNO) capacity for the armed forces will include all components for defensive measures in the electromagnetic spectrum and cyberspace. Whatever the future for Sweden is in the area of cyber, the development will require new methods and processes in building capabilities.

The Nordic Countries and Their Potential for Cooperation

Defence cooperation between the Nordic countries and Nordic defence cooperation in the area of cyber have world class potential, because the Nordic countries share

1) **A common culture** In the Nordic countries, there is a similar style of thinking and acting in the information society. The level of information technology usage is high, and the widespread access to information services tells of the common practices in the Nordic countries to build a characteristic societal model. In addition, there is enthusiasm for cyber in the armed forces. Shared cultural elements include the lack of corruption, a will to improve the efficient use of resources, a will to perform high quality activities and to provide practical solutions to the challenges of cyber, as well as a desire to be operationally more efficient than today. The Nordic countries share a common culture and know-how which makes cyber cooperation possible.

2) **Dependency** Geography and technology connect the Nordic countries. A great deal of economic factors relate to geography like the Baltic Sea and the northern regions. The societies of the information age are dependent on electronics, programs and products based on information technology and services. The dependency of the economies of the Nordic countries on a functioning cyberspace increases the possibilities for cyber cooperation.

3) **Expertise** All Nordic countries possess world class cyber structures and cyber expertise, no matter how it is measured: infrastructure, the level of use, networking or dependency. In all these areas the Nordic countries are among the top ten in the world. However, this expertise requires continuous practical support.

4) **Common topics** There is much talk about cyber among politicians, bureaucrats and entrepreneurs. In the meanwhile, the jargon of cyber is becoming harmonized. The concept of cyber is broad enough to discuss. However, this conceptual scope can lead to confusion as to what is really meant by cyber. Language has other functions than merely speech. The potential for cyber cooperation is increased through the dispersion of information, increased understanding, the display of emotion, the effect on the audience and even the avoidance of silence.

5) **Common political will** The Nordic countries have shared interests in the area of cyber. The challenge may be the traditional security paradigm, which builds border fences. A challenge for cyber can be, for example, the political boundaries of NATO cooperation, which can be considered a hindrance to cooperation. Regardless, Norway has made proposals for cooperation in the area of cyber.

6) **Window of opportunity** Cyber is a current topic. However, in the future cyber issues may not enjoy such popularity. The window of opportunity for the development of cyber cooperation is at hand. Technology creates possibilities for change but technology itself is going through a constant change.

What could NORDEFCO cooperation be?

This study supports the idea that cooperation in the area of cyber is possible in principle because it could benefit all of the countries involved. The cooperation should be practical, however, in accordance to political positions, which does not exist today. This research encourages the Nordic countries to further explore possibilities for cooperation in at least – but not limited to – the below mentioned areas.

1) **Leadership development** The prerequisite for all change is genuine leadership that comprehends the current and future character of life in its full scale in cyberspace. Leaders in particular, on different levels, demonstrate through example whether countries have sufficient will, respect and right attitude to reach concrete forms of cooperation. Leading is inspiring. Creating a common goal is to lead. This can take the form of joint statements. The leadership of cyber requires more than just talk; it also requires joint statements, plans, their implementation and joint action. The fostering of shared understanding of leaders should be encouraged. An initiative should be taken to promote cyber discourse. Leadership skills can be created together in the Nordic countries.

2) **Exchange of information** Each Nordic country is following events taking place in cyberspace. Each Nordic country is independently developing cyber structures. Information could be exchanged between the national CERTs. In addition, information could be exchanged between the monitoring units of each country's armed forces. The "lessons learned" method could be a very useful practical method to share cyber information/knowledge.

3) **Common cyber strategy** If the countries do not share a common goal, it is difficult to develop sustainable cyber activity. Cyber challenges are not country specific and therefore, there is a need for wider cooperation. One possibility is to develop a common cyber strategy.

4) **Common exercises** Interoperability is a requirement for Nordic cyber cooperation. There may be a language gap between the leadership and the implementation in cyber; different levels deal with different issues and use different language(s). There are no functional standards. In the area of cyber, this could signify that the means to react to

cyber alarms differ from one another in different countries. Nor are technical systems necessarily inter-functional; there is a need for inter-compatible procedures. Linguistic, procedural and technical compatibility can be developed, for example, via the exchange of information and, in particular, through practice. The Nordic countries have already participated in international cyber training. The implementation of joint Nordic cyber defence exercises would therefore be a rather easy path toward practical cooperation in the Nordic countries.

5) **Common organization** Cooperation in the area of cyber cannot take place solely in a military context. A wider cooperation is needed of countries and authorities. This could be a) the establishment of a common Nordic CERT, and b) the positioning of contact persons in neighbouring countries' CERTs or cyber-centres.

6) **Legislation** Researching the possibilities for the standardisation of legislation is based on cooperation and the development of compatibility. The challenges of legislation arise from the "grey area" which lacks clear legislation.

7) **Development of know-how** The core of cyber security is not so much technological questions than personnel questions. Know-how can be found, for example, in voluntary organisations, whose activities should also be supported. Individual know-how, and the statistics of how many experts can be found and the extent of their expertise has not yet been established. Cyber is personnel, not tech-heavy. The know-how of the individual is important. Professional military culture is not necessarily the best atmosphere to solve cultural challenges concerning cyber personnel. All this means creating the right atmosphere, not only among national cyber experts, but to set the stage for Nordic cooperation.

8) **Research cooperation** Relatively new, yet not sufficiently examined areas can be found in cyberspace, such as legislation, cyber security software, procedures to share information, and social media. Mapping out common research interests and starting up research projects is a potentially easy path to cooperation.

The most important requirement for cooperation, in addition to motivation, is trust between the different parties. The depth of Nordic and NORDEFCO cooperation depends on whether the parties involved trust one another and their ability to envision the cooperation on a broader scale than in the past.

Introversion or traditional Cold War thinking in which state borders had greater significance and in which physical security factors were highlighted does not necessarily work in the culture of cyberspace. Cooperation in cyberspace means that the antiquated competitive attitude should be abandoned, because it does not answer the challenges and threats of cyber. A good example is virus laboratories, which share new information immediately and do not withhold it from each other.

How new analytical concepts, operational models and tools help the Nordic countries and their Defence Forces to sustain cyber security in the field of defence is a question yet to be answered. However, in order to continue being the best countries in the world to live in, this study encourages further discussion on matters such as innovation, will, attitude, trust, and practical cooperation.

Jari Rantapelkonen
Professor
National Defence University
FINLAND

Mirva Salminen
Doctoral Candidate
University of Lapland
FINLAND

Introduction: Looking for an Understanding of Cyber

Jari Rantapelkonen & Mirva Salminen

The Fog of Cyber Defence is a book about cyberspace, cyber security and cyberwar. This introduction, as well as the whole book, is untangling the ties of the Nordic states with the important, yet complex and foggy phenomenon of cyber. It offers insights into the important themes of cyber from multiple perspectives.

The Main Argument of the Book

The future is here, but it is unclear. This thought sits well with the phenomenon of cyber, because cyber is both future and present. Future, for the fog that obscures our understanding of it, and present, for we are encircled by it and working with it.

The Fog of Cyber Defence is adding important Nordic perspectives into the ongoing discussion about cyber security and, hopefully, creating room for the deepening of co-operation amongst the Nordic states. The book does not claim to present what cyber is or to provide real facts about it. Instead, the articles in the book contribute to the debate over the implications of cyber for the national security and the armed forces. The authors, who come from various professional backgrounds, appreciate and welcome further discussion and comments on the very important themes that impact our everyday lives.

The authors of the articles agree that cyberspace is important for the wealth of the state. Moreover, we claim that cyberspace is vital for the Defence Forces in conducting land, sea, air, and joint missions abroad and at home. We believe that cyber security delineates national security, especially in the high-tech states. If the Nordic states wish to be prepared for the future, enhanced co-operation is needed. This applies to all levels of co-operation from global politics to volunteer services. We agree that cyberwar should be taken seriously. However, and especially because so many contemporary actors seem to focus merely on attacking capabilities in cyber, we argue that the current trends, as well as the future, need to be scrutinised more carefully in order to acknowledge the importance of defensive cyber capabilities.

In the end, we can hopefully agree on the main argument of the book: the fog of cyber defence needs to be better investigated and understood. This is important if the Nordic states wish to enhance their operating capability in cyberspace.

The Fog of Cyber Defence acknowledges that the phenomenon of cyber is unclear and uncertain. The book thus borrows an idea from Carl von Clausewitz, who argued that war is an area of uncertainty. Cyber as a domain, as well as actions in, across and on the borders of it are characterised by omnipotence, complexity and unpredictability. In the face of the seeming chaos there is an enhanced need to categorise and organise the domain in order to

improve one's capabilities to act in it in a planned manner. In discussing what cyberspace is, how cyber security is to be arranged and/or cyberwar waged, one soon notices that in cyber defence rhetoric and action, hype and real, virtual and physical are different realities. These realities should be set in a dialogue. On paper, we may have many brilliant ideas about cyber strategy, cyber espionage or hacking in the battlespace. However, the establishment of a unified cyber defence that provides security for states and their citizens is a challenging practice because security is, first of all, a feeling – not a machine, nor a system.

In cyberwar, one of the biggest issues for the armed forces is the basic question of what war is. Guns kill, bits and bytes do not – or they have not killed thus far. This presumption has been challenged, for example, by Stuxnet which blurred the limits and borders of war. Therefore, *The Fog of Cyber Defence* asks what the relationship between guns and bits, soldiers and cyberwarriors, the armed forces and civilian institutions, plans and actions, and/or strategic and tactical levels is. The book calls for an examination on the aforementioned borderlines. The challenge offers a great opportunity to create a better future. We need an improved understanding of the ambiguous phenomenon of cyber, because there is too much uncertainty inherent in the practices on cyber defence and cyberwar. The challenge is also the reasoning behind the book's metaphorical cover with a foggy background and an unclear title: *The Fog of Cyber Defence*.

The Purpose of the Book

The Fog of Cyber Defence is based on the authors' voluntary contribution. The authors wish to add their own share into the discussion revolving around cyber security.

The book informs its readers about the active and significant role that computers play in the Nordic states and their growing importance in the Nordic way of life. Specifically, it deals with the issues of cyber security that still some years ago were understood as distant hype or as the prerogative of professionals and experts. Nowadays, they are no longer only future but also reality, that is, they are present in the lives of soldiers and ordinary citizens alike.

Information technology has promoted socio-economic development and provided new services. It has changed the ways of business and the exchange of information between people, individuals, organizations, businesses and governments1. We are ever more dependent on computers and networks that provide, for example, energy, transport, finance, e-commerce, and health. Information infrastructures interconnect and affect human life increasingly via cyberspace. This book aims at creating greater public awareness of the discussion over cyber security. It calls for the information societies to rethink their vulnerabilities that raise new security concerns.

The Fog of Cyber Defence provides also a chance for politicians, business, military and ordinary citizens to learn more about the complexity of cyberspace and its comprehensiveness. Growing technological interdependence relies on a complex network of information infrastructures.

[1] UN GA (2004). Creation of a global culture of cybersecurity and the protection of critical information infrastructures. A/RES/58/199, 30 Jan 2004.

The Fog of Cyber Defence clearly shows the evil face of cyberspace, that is, cyber threats. Cyberspace is not only a gateway to a better future, but also full of criminality, espionage, and warfare. It is an interconnected space and a world we live in without clear borderlines and responsibilities.

The importance of cyberspace and the need to defend oneself against cyber threats have become huge questions in the modern era. As the Nordic states and their militaries rely more on computers, networks and artificial intelligence, there is an enhanced need to secure capabilities and services that are located or used in cyberspace. We depend more and more on cyberspace, and that space must be defended as all Nordic states manifest to believe. The protection of states, organizations and individuals requires co-operation – not only at the national level, but also internationally. A number of states have already declared that they prepare for cyberwar. With regard to this, the book provides insights into the problematic nature of cyberwar.

All in all, the book serves as an unofficial forum for discussing cyber defence. Yet, it has been written in the spirit of NORDEFCO to facilitate further discussion and co-operation under its umbrella. Even if *The Fog of Cyber Defence* contributes to the NORDEFCO in facilitating the uttering of thoughts on cyber security, it does not represent the opinion of NORDEFCO or its participant nations. Nor does it suggest future areas of co-operation, but primarily provides food for thought.

The main argument of the book recognises the complex nature of cyberspace and cyber security. In order to understand the phenomenon better, *The Fog of Cyber Defence* has called for and respects the various perspectives on, methods for and cultures of international cyber security that are presented by the authors. Understandably, the book and its articles do not cover all of the important areas of cyber security, but only bite a few pieces of the complex cyberspace.[2]

The book also recognizes and follows the United Nations resolution 58/199 which "*Encourages* Member States and relevant regional and international organizations that have developed strategies to deal with cyber security and the protection of critical information infrastructures to share their best practices and measures that could assist other Member States in their efforts to facilitate the achievement of cyber security.[3]"

To state it in a precise manner: the book represents solely the personal opinions of the authors. It does not represent the official views of National Defence University, the Finnish Defence Forces, Finland or any of the other Nordic states, or institutions the authors may have an affiliation with. All of the articles either introduce personal research findings or represent personal opinions.

[2] Nordefco (2011). GUNOP – Guidelines for NORDEFCO military level operating procedures. Ver 2.0, Sept 2011, p.6-15.
[3] UN A/RES/58/199 (2004) Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures, 30st of January, 2004.

Contents of the Book

The book comprises three parts: Cyberspace, Cyber Security and Cyberwar.

Part I: Cyberspace

Insights into Cyberspace, Cyber Security and Cyberwar in the Nordic Countries is a comparative article that scrutinises similarities and differences between the Nordic states in their relation to cyberspace and cyber security. Professor **Jari Rantapelkonen** from National Defence University and Major **Harry Kantola**, who is both a teacher and a Doctoral Candidate at National Defence University, argue that all the Nordic states and their armed forces are willing to develop military capabilities both to defend and to attack in cyberspace. These efforts are challenging, firstly, because of the traditional political choices between competition and co-operation. Secondly, building security in cyberspace requires an improved understanding of what war in cyberspace is and what is the meaning of cyberspace for war.

Sovereignty in the Cyber Domain is written by **Topi Tuukkanen**, who is a senior staff officer serving in the Finnish Ministry of Defence. He contributes to the theorising about the very basis of cyberspace: What do borders signify and who has the control in cyberspace? Commander Tuukkanen's article raises other important questions too, such as: can the nation state acquire some level of control or sovereignty in cyberspace, and what is the role of the state acting in cyberspace?

Cyberspace, the Role of State, and Goal of Digital Finland is a thoughtful article by **Jari Rantapelkonen** and **Saara Jantunen**. Professor Rantapelkonen and Doctoral Candidate Jantunen, both from National Defence University, analyse the official government program leading to Digital Finland, and ask whether the state is the best entity in lead of digitizing cyberspace? The authors claim that the question is relevant because of the very nature of the domain, cyberspace.

Exercising Power in Social Media shows how social media can be used as a tool in a political struggle. The article scrutinises the question in the light of the electoral protests during the 2011/2012 elections in Russia. In the article, **Margarita Jaitner**, Doctoral Candidate from Karlstad University, focuses on how a government can counter an opposition growing within social media. She introduces and categorizes a number of possible counteractions basing on the application of Joseph Nye's theory of hard and soft power. She also suggests that there are several possible ways to counteract a movement which arise within the situation.

Victory in Exceptional War: The Estonian Main Narrative of the Cyber Attacks in 2007 is an article in which **Kari Alenius** focuses on the large-scale cyber attacks Estonia fell victim to. For some the cyber-attacks mark a milestone in modern warfare. Docent of the University of Oulu, Alenius's study does not declare whose perspective on the attacks is "right" and whose is "wrong". Instead, he analyses published Estonian interpretations of what happened and argues that the most essential element in the popularisation of the attacks was that the events were seen as a war with all its

classical characteristics. In this context, actions of one's home nation were perceived as a successful repulse to enemy attacks and a foreign country (Russia) was perceived as an attacker.

Part II: Cyber Security

The Origins and the Future of Cyber Security in the Finnish Defence Forces is an interesting article from **Anssi Kärkkäinen**. Captain Kärkkäinen from Defence Command Finland is also a Doctoral Candidate at Aalto University. His article reviews the development of the Finnish Defence Forces' (FDF) cyber security over the past few decades. The article depicts this progress from information and network security to modern cyber defence capabilities. The role of FDF in the national cyber defence system is also discussed, as well as the development of FDF cyber capabilities in the near future.

Norwegian Cyber Security: How to Build a Resilient Cyber Society in a Small Nation is written by **Kristin Hemmer Mørkestøl**, who is a senior adviser at the Department of Security Policy in the Norwegian Ministry of Defence. In her article, Mørkestøl provides an insight into the Norwegian process towards increased robustness in cyberspace. Her aim is to share lessons learned which may be of use for other smaller nations facing similar endeavours, such as raising awareness on the need to clarify cyber roles and responsibilities within government, as well as the importance of cyber competence amongst decision makers. She also challenges the reader on cyber issues of national and international relevance that deserve further exploration, such as the application of international law and the use of worst-case scenarios for better preparedness planning in the cyber domain.

Cyber Security in Sweden from the Past to the Future is written by **Roland Heickerö**, Associate Professor from the Swedish National Defence College. Pioneering technologies such as Internet and mobile telephony provide people with enhanced opportunities to communicate and spread information. In order to handle the associated threats, all high-technological nations develop doctrines and the capacity to protect and defend functions that are important to society and critical infrastructure. Heickerö's text provides examples of present organisations and activities that handle cyber security at the Swedish national level. It also provides a historic perspective to the issue, and examines what cyber security is heading towards in Sweden.

In A Rugged Nation, the Finnish Security Strategy for Society dated in late 2010 is analyzed from the perspective of cyber threats in 2012. **Simo Huopio**'s, who is a researcher at the Finnish Defence Forces Technical Research Centre, conclusions are clear: cyber threats cannot be treated only as an isolated phenomenon. Instead, they need to be analysed in conjunction with other major threats in which the cyber domain plays a significant role as an enabler. In order to counter cyber threats resiliently information systems have to be specified, procured, produced and used in such a way that everybody participating in the process shares a common vision on what is to be protected, in which way, and feels proud of being part of the process. The key themes of the article are taken from the Rugged Software Initiative

and extrapolated from software application development to critical infrastructure protection.

Contaminated rather than Classified: CIS Design Principles to Support Cyber Incident Response Collaboration is a study executed by **Erka Koivunen**, Deputy Director in charge of Incident Management at Finnish Communications Regulatory Authority. Many attacks in the cyber domain seek to exploit weaknesses in Communications and Information Systems (CIS) hence posing a threat to the very technical foundations of networked data processing and to the information society at large. To play it safe, one needs to operate in specialised computing environments that expose as little attack surface as possible while still providing enough means to observe the true behaviour of malicious payloads. The Nordic states have taken the bold move to create a network for inter-Computer Security Incident Response Team (CSIRT) collaboration on a classified level. This paper outlines the design principles adopted by CERT Finland for its internal CIS and draws parallels to the Nordic CERT Network, or S7 network.

Part III: Cyberwar

Cyberwar: Another Revolution in Military Affairs? is written by Major (G.S.) **Tero Palokangas**, who currently participates different Finnish Defence Forces' research and development programs that focus on the digitalization of the Finnish Army. The author challenges the latest thoughts about cyberwar as a kind of revolution in military affairs or as a domain of war by itself. He argues that the best way to survive in cyberwar is to develop own C4-systems in a determined way, so that one can be certain and confident about all processes and applications in use. Information assurance and security must be tightly connected with cyberwarfare. Without vulnerabilities there are no cyber threats – excluding the human nature and behaviour, which remain to be the most important threats in future cyberwarfare.

What Can We Say About Cyberwar based on Cybernetics? is an interesting but rare view provided by Lieutenant Colonel (Ret.) **Sakari Ahvenainen**, who is a general staff officer and a freelance information warfare and network centric warfare researcher since 1990's. His article looks down to the basics of cyberwar, meaning mainly cybernetics, but also cyberspace as a new global infrastructure and cyberwar as a global level of warfare. Types and levels of cybernetic information and their importance to cyberwar are studied. Human and computer as a cybernetic systems and targets of cyberwar are also examined. Ahvenainen finds eight logical types of cyberwar, and claims that computer programs and integrated chips added with human understanding are at the hearth of cyberwar.

The Emperor's Digital Clothes: Cyberwar and the Application of Classical Theories is written by Captain and D.Soc.Sc. **Jan Hanska** from National Defence University. The author refers to classical military theorists and argues that even if cyberwar is something new in itself, it need not to be part of any revolution of military affairs. Instead, it is a sign of normal evolution. War always reflects the characteristics of the societies waging it. Therefore, the ideas of the classical thinkers need to be restudied,

deconstructed and applied in the new contexts. Ways and means become altered, but war itself remains perpetually a part of the human condition.

Theoretical Offensive Cyber Militia Models is written by Dr. **Rain Ottis**, who is a post-doctoral researcher at the University of Jyväskylä and also lectures at Tallinn University of Technology. During 2008-2012 he was a scientist at the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia. Ottis's article explores the various forms of offensively oriented volunteer groups (cyber militias) taking part in modern cyber conflict. He proposes three theoretical models for such groups and analyzes their attributes, strengths and weaknesses.

Offensive Cyber Capabilities are Needed Because of Deterrence is written by D.Mil. Sc. **Jarno Limnéll**, Director of Cyber Security in Stonesoft Corporation. He argues that within the next couple of years the world will experience more intentionally executed and demonstrated cyber attacks. At the same time, the development of offensive cyber weapons will become fiercer and publicly more acceptable. Limnéll analyzes the importance of offensive cyber capabilities to nation states and predicts the future construction of the cyber deterrence in the world.

Threats Concerning the Usability of Satellite Communications in Cyberwarfare Environment is an article written by Professor **Jouko Vankka** and Doctoral Candidate **Tapio Saarelainen**, both from National Defence University. The Nordic states often participate in international missions that rely on satellite communications. In military operations, satellite communications offer a network system that can be constructed fast, does not require land-communications network system, and offers a wide variety of services to military troops in peace supporting and military operations. The article discusses three possible threats concerning the usability of KFOR satellite communication systems in the context of cyberwarfare; namely, physical weapons, logical weapons and network attacks. The article also proposes methods applicable when facing these threats.

The Care and Maintenance of Cyberweapons is written by Doctoral Candidate **Timo Kiravuo** and D.Sc. (Tech.) and post-doctoral researcher Mikko Särelä, who both come from Aalto University. Prior to joining the university, they both worked in the private sector. In their article, they investigate how a modular weapon system can create offensive cyber capability. Their main argument is that cyber capability is based on the continuous identification of gaps within the system, attacks against them and the ability to compile a weapon from the available components in each necessary situation.

The Exploit Marketplace is an article written by **Mikko Hyppönen**, F-Secure's Chief Research Officer. Weaponized exploit code to attack vulnerabilities in operating systems and applications have become the everyday trading goods of the cyber armament industry. Several boutique companies go out of their way to find bugs that can be exploited and turned into security holes. Once being found the bugs are weaponized so that they can be abused effectively and reliably. These companies also make sure that the home company of the targeted product will never learn about

the vulnerability - because if it did, the exploit code would become worthless to the vendor.

Questions for Further Research

The Nordic states – Iceland, Denmark, Finland, Norway and Sweden – are seeking security in cyberspace. States, as other actors in international politics, are looking for co-operation, yet competing for power and control. Regardless of different rhetoric, they are seeking to extend sovereign control into cyberspace. One of the challenges for states is to find opportunities for co-operation when cyberspace cannot be controlled "in the old style", that is, with the tools of political realism.

Interdependencies in cyberspace and cyber security vulnerabilities are numerous. This can act as a useful basis for furthering co-operation. The question is what kind of co-operation is needed to tackle the aforementioned challenging issues. Other questions, such as those of deterrence, laws of armed conflict and prevention, have traditionally dominated the national agendas. These questions have not been solved and are still relevant, but the agendas need to be augmented with the issues of cyber.

The articles point out yet another interesting, difficult and necessary question, which is the malicious activity in cyberspace. Foggy areas include, but do not necessarily limit to, the focus, duration, and the effect of cyberwar and cybercrime. These areas need to be clarified – also in the discussion that takes place within and between the Nordic states.

Ultimately, cyber defence is not only about technology. Ethics, norms, and the ways of dealing with the important issues of cyber security are questions that need to be agreed on in co-operation between persons, institutions, militaries, states, and international organizations. Given the complex natures of cyberspace, cyber security and cyberwar, the topic of cyber defence requires further discussion in the Nordic states.

Acknowledgements

We would like to thank J5 Finnish Defence Command for providing us an interesting research project in the spirit of NORDEFCO and in accordance with the best academic practices. The complex topic was a challenge; as was the time-space to think about the many issues of cyber defence. Fortunately, the professionals volunteered to contribute to one of the most important topics of the modern era.

We also appreciate National Defence University for its willingness to publish the book – especially, the people who serve at the Department of Leadership and Military Pedagogy, but also those at the Department of Operations and Tactics.

The compilation of this book was aided by many. One of the crucial applauses goes to Tannisen Säätiö which provided economic support to bring these thoughtful articles into daylight.

In the end, the book project would not have been possible without the most important: persons, thinkers, authors of the articles – these wonderful people. During the project, we editors have encountered and been privileged to work with so many professionals on cyber. To all of them we owe a warm thank you for contributing to the debate over cyber.

Part I:

Cyberspace

Insights into Cyberspace, Cyber Security, and Cyberwar in the Nordic Countries

Jari Rantapelkonen & Harry Kantola

Abstract

Insights into Cyberspace, Cyber Security and Cyberwar in the Nordic Countries is an article that shows how advanced the Nordic countries are in relation to cyberspace. The article discusses narratives that show how the western countries and their militaries are willing to develop not only defensive, but also offensive capabilities in the field of cyber security. Simultaneously, these efforts challenge the existing understanding of what war –and cyberwar – is, and what it is not. Like other spaces, cyberspace will be used for the purposes of war, not necessarily only for cyberwar as such. Therefore, it is suggested that cyberwar should not be defined as a concept of war, but treated as an open phenomenon. This article suggests that the Nordic countries reconsider the concept of resilience and seek cooperation to face the challenges of cyberspace.

Keywords: cyberspace, cyberwar, cyberhype, reality, phenomenon, the Nordic countries, resilience, cyber resilience

The essence of technology… is the danger.
Martin Heidegger, 1955

Introduction: Waging Cyberwar

Somewhere out there, a cyberwar is going on – as we can read in tweets and news. In 1986 the allegedly first virus, "Brain.A", infected personal computers. Two years later, the "worm" Morris became one of the first malware programs distributed via Internet. Roughly two decades later, in 2007, "zombies" attacked Estonia: "infected" computers used botnets to disturb and disrupt Estonian governmental and other important Internet providers. Then, in 2010, a "worm" called StuxNet was the first malware able to do physical damage to an Iranian nuclear enrichment plant. The most recent story on cyberwar that hit the newspaper headlines in early 2013 is the "Red October". This is not a fictitious modified Russian typhoon class submarine, as mentioned in Tom Clancy's novel "The Hunt for Red October". Instead, "Red October" or "Rocra" is an "advanced cyber espionage network that has been active for at least five years and is targeting diplomatic and government agencies"1. Yet, there is no compelling evidence to show who is behind this latest cyber event – which reveals one of the reasons why cyber security is difficult to deal with and raises the question whether cyber security and cyberwar are real or hype. According to Martin Heidegger2, the most probable threat to man in the first instance is not the possibility of cyberwar or even lethal machines and the apparatus of technology; the actual threat has already affected man in his essence.

[1] http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_Operation_Red_October_an_Advanced_Cyber_Espionage_Campaign_Targeting_Diplomatic_and_Government_Institutions_Worldwide
[2] Heidegger (1977), p.28.

Going back to history, one may argue that cyberwar came along with the development of technology, cybernetics and cyberspace[3]. Among others, the subject has affected the Nordic countries, as well as Estonia. Increased attention from security authorities and companies dealing with cyberspace has resulted in increasing discussion about cyberwar and cybercrime, but not necessarily in improved cyber security.

In 1993, in the widely cited RAND paperback "Cyberwar is coming!" John Arquilla and David Ronfeldt predicted that the importance of cyber is going to increase and that it will have an impact on warfare. Since then, not only in the US military establishment, but all around the world in high-tech societies, such as the Nordic states, cyberwar has been discussed and accepted, debated and denied, and also exercised.

Now, twenty years later, we can conclude that cyberspace is an everyday domain for any kind of human activity from social activities to business. It also includes the military activities and acts as a space for crime. Lately, the concept of cyberwar has generated a growing number of academic research projects to find out how to utilize it, but also how the threat of cyberwar could be eliminated. Nevertheless, future cyberwar needs yet to be researched thoroughly and the concept to be secured. Considering the Nordic countries, we see that there are few open cyber security research projects to attend and, as a matter of fact, the Nordics have no common ventures at all.

Over the past years, there have been predictions of "nationwide" power blackouts, planes falling from the sky, trains derailing, refineries burning, pipelines exploding, poisonous gas clouds wafting, and satellites spinning out of orbit – events that would make the 2001 terrorist attacks pale in comparison.[4] This "Digital Pearl Harbor" could take place anytime, as some high-level national security personnel, like the U.S. Defense Secretary Leon Panetta, have warned. [5] Even though none of these predictions has come true yet, there is a dark side to cyberspace and there is room for destructive potential[6]. Technology, according to Heidegger, might be a supreme danger to man.

The aforementioned leads to the question whether cyber is yet another element of regular evolution or a revolutionary change in warfare. After all, if cyberwar is defined as war, it is reasonable to argue that some basic matters – such as actors, resources, skills and methods – have changed. Currently, unlike in the age of large-scale mass warfare and nuclear weapons, cyberwar is accessible to any "cybernerd" with enough skill and an access to a computer

[3] Cyberspace has many definitions, and there is no consensus on what cyberspace exactly is. It is arguable that modern cyberspace emerged due to the convergence of three events: the introduction of the personal computer in the mid-70s, the Internet in the early-80s, and the worldwide web protocol in the late-80s. In general terms, cyberspace can be understood as the collection of computing devices connected by networks in which electronic information is stored and utilized, and communication takes place. Another way to understand the nature of cyberspace is to articulate its purpose: the processing, manipulation and exploitation of information, the facilitation and augmentation of communication among people, and the interaction of people and information. Both information and people are central to the power of cyberspace. A third definition seeks a better understanding of what cyberspace might be by identifying its salient characteristics. Look at these Clark, David (2010). Characterizing cyberspace: past, present and future. (see http://web.mit.edu/ecir/pdf/clark-cyberspace.pdf). Yet another view argues that cyberspace consists of physical, logical and social layers (see. http://www.fas.org/irp/doddir/army/pam525–7–8.pdf). In this introduction, cyberspace as technological and social space relies much on the definition of Ottis and Lorents. Ottis, Rain & Lorents, Peeter (2010). Cyberspace: Definitions and Implications. Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia. Available at http://www.ccdcoe.org/articles/2010/Ottis_Lorents_CyberspaceDefinition.pdf

[4] Clarke & Knape (2010).

[5] Rid (2012).

[6] Heickerö (2013).

and Internet. On the other hand, how do these "cybernerds" differ from regular insurgents? While insurgents gain access to powerful weaponry, information, and skills to use them, "cybernerds" gain access to powerful computers, information, and skills to use them.

Time for a Reality Check?

During the past twenty years, there have been practical incidents, for example, Estonia 2007, Georgia 2008, Stuxnet 2010, and Red October 2012. Nonetheless, a request "for a reality check" can be done: cyberwar is still more hype than hazard. With regard to the definition of an act of war, war has to be potentially violent; it has to be purposeful; and it has to be political. In an article published in Foreign Policy in 2012, Thomas Rid claims that "the cyber attacks we have seen so far, from Estonia to the Stuxnet virus, simply don't meet these criteria".[7]

In comparison to war (a conflict between states) one of the new features in cyber conflict is that war in the cyber domain can be waged by amorphous groups of disaffected young hackers such as Anonymous and LulzSec. Such groups have cracked the websites of, for example, government security contractors, the Church of Scientology, Sony, Amazon, Visa, MasterCard and the FBI. Even though these acts are considered cyber criminality, they have the potential to turn into cyberwar, if political will and violence are added to their actions. This connection has obviously been very difficult to understand for the Cold War warriors. It poses a challenge to the mental models of the Cold War era but also to the citizens of the information age, since the newfangled phenomenon of Anonymous and the like, born in cyber domain itself, struggles to make sense altogether.

Olson explains how a loosely assembled group of hackers scattered across the globe form a new kind of insurgency. It is even more difficult to understand how warriors and wars can "spontaneously emerge from a place that most of the Internet's travelers would never know existed." These groups grow almost organically, always rapidly, and change their character over time. Someone who has never heard of Anonymous cannot understand this kind of cyber insurgency and how it can be considered war.[8]

The trend has developed over the past decade when the rise of insurgents and non-state actors in war, and their readiness to use irregular methods of fighting, has led the commentators to speak of 'new wars'. They have assumed that 'old wars' were waged solely between the states, and were accordingly fought between comparable and 'symmetrical' armed forces. However, if we read Clausewitz's final section of "On War" and his opening chapter that describes war as "a strange trinity" of three elements – hate, chance and reason – we have to admit that operations in cyberspace conducted by groups who are motivated, skilled and aggressive against their adversaries constitute a war. The future is unpredictable, and our present security condition may as well become a great deal worse than it is today.[9]

This raises the question of how serious phenomenon cyberwar is for the Nordic countries. Are the possible consequences as severe as the consequences of conventional war? "The

[7] Rid (2012).
[8] Olson (2012).
[9] Gray (2009).

importance of cyberspace in conflict is not whether computer networks are involved as a separate domain, but where, how, and to what significance for the outcomes", argues Chris Demchak, who advocates discussing cybered conflicts, a term that is more suitable for the national security of high-tech countries, rather than cyberwar.

Demchak explains that "Any given conflict can involve all sorts of systems of people, things, processes, and perceptions that are computer-related but not necessarily purely computerized. Phishing can be an attack even if it simply sends information to bad actors through the foolishness of the email recipient. The purely cyber portion could constitute a preparatory phase, a main avenue of attack, central campaign element, a large scale deception and espionage operation, an episodic enabler, a foregone set of activities, or all of these at different times in a long term cybered conflict. In a cybered conflict, many key activities occur only partly purely inside networks. At the end of the day, a 'cybered' conflict is any conflict of national significance in which success or failure for major participants is critically dependent on computerized key activities along the path of events."[10]

There is no unanimous concept of cyberwar. Nor there is a consensus, international or even national, on which hostile actions in cyberspace would be recognized as acts of war. Therefore, it depends on the combination of perspectives and interests whether cyberwar is regarded to be a war or an independent struggle in cyberspace; whether it is the same as the Banana Wars; or whether cyber plays a similar role to logistics in conventional warfare. There are potentially insurmountable issues around cyberwar. Cyberwar is complex, ranging from a phenomenon to a threat. Doctor Jarno Limnéll puts it nice and neatly by arguing how difficult it is to work with security issues because "no-one can say, what kind of cyberweapons different countries have developed and what kind of threats they create"[11].

Security is a feeling, not a fact – and this makes the scope of cyber as a challenge more difficult to cope with. The difficulty of defining whether cyberwar is a war or not also results in difficulties in characterizing what constitutes a weapon in cyberspace. A regular weapon is meant to shoot and kill; computers do no such thing alone. However, security being foremost a feeling grounds particularly true, as according to a McAfee study "57 % of global experts believe that an arms race is taking place in cyber space".[12] According to Singer and Wright there is a global proliferation going on within cyber, where it is estimated that over a hundred countries have developed cyberwarfare capabilities.[13]

Cyberwar certainly depends on its definition and its relation to the nature of military power. Whether our focus is on numerical strength, technological pendulum, or non-material factors, it defines the contents of war and cyberwar. The context defines war, which means that war can mean different things in different contexts. One can speak about conventional large-scale ground war, air war, humanitarian war, and war on terror, cyberwar in high-tech societies, etcetera. War depends on the mission and tasks that can range from killing and destroying to searching, taking and holding. Defending networks from hackers shows how diverse cyberwar can be depending on the particular technical environment. Who, in this

[10] Demchak (2010).
[11] STT (2012).
12 Mcafee *Cyber-security: The Vexed Question of Global Rules, available at http://www.mcafee.com/us/resources/reports/rp-sda-cyber-security.pdf?cid=WBB048*
[13] Singer & Wright (2013).

case, is a soldier, and what is a weapon? Kaspersky, for instance, limits his definition of cyberwar to the use of cyber weapons to cause physical damage[14]. Mikko Hyppönen from F-Secure agrees that cyberwar is not taking place until critical infrastructure is threatened.[15] War is also a narrative; a power to use terms, define contents and to refer to relevant elements.[16]

Great efforts have been put into defining the elements of cyberwarfare, both in and outside the Nordic countries. The U.S. National Research Council of the National Academies, for example, recommends a basic framework for legal analysis in which potential cyber attacks "should be judged primarily by the effects of an action rather than its modality." Furthermore, it addresses the implications of such framework by using the Article 51 of the UN Charter for attacks prior to an acknowledged armed conflict, and the standard law of armed conflict (LOAC) for an acknowledged conflict. Currently, the U.S. military is developing a doctrine that will distinguish between the role of cyber attack and the intelligence role of cyber exploitation. Terminology to describe cyberspace operations in general, as well as the specific concepts of attack, defense, and the electromagnetic spectrum, still varies among the U.S. Services.[17]

How seriously the Nordic countries should prepare for engaging in cyber conflict depends on how cyberwar will be defined. Will cyberwar have enough importance to push for new definitions of war and deterrence? This depends on who will have the power and the will to draft definitions. It also depends on who will benefit from the new concepts and be able to use them for his or her purposes.

Whatever the reality is, whether cyberwar is an act of war or an act of information flow, the phenomenon demonstrates a need to address multiple cyber security challenges. The state has to be a credible actor in cyberspace, because real life has a cyberspace dimension – and cyberspace is part of the real life. In the Nordic countries, cyber security has now been identified as a concern for both national and international security for a good reason: “Western governments are unsure of how far they can go in patrolling the Internet without infringing on their citizens’ freedom[18]”.

Cyberspace – the Nordic Countries as Networked States

Cyberspace is increasingly important for the economies of the Nordic states and for the quality of life that combines equality and social well-being of people, businesses and authorities. The Global Information Technology Report from 201219 confirms that the Nordic countries and the Asian economies are well ahead in adapting and implementing information and communication technology, promoting growth and development. Sweden ranked first on the worldwide Networked Readiness Index (NRI). Finland was third followed by Denmark

[14] Stiennon (2012).
[15] http://news.techeye.net/security/cyber-war-is-now-cleaner-but-far-more-dangerous
[16] Also, military power can have different meanings in different contexts. See also Biddle (2004).
[17] Owens, Dam & Lin (2009).
[18] Dempsey (2013).
[19] http://reports.weforum.org/global-information-technology-2012/

as fourth, and Norway achieved the seventh place putting the four Nordic countries into the top ten on the NRI.[20]

Today, cyberspace partly defines the structure of the Nordic welfare society. The Nordic countries are places "where the Internet and its associated services are accessible and immediate, where people and businesses can communicate with each other instantly, and where machines are equally interconnected with each other" and where "[t]he exponential growth of mobile devices, big data, and social media are all drivers of this process of hyper connectivity." This reliance on virtual connections and services increases growth and well-being particularly in high-tech countries.[21] These might be reasons why cyberspace has become so important for the Nordic countries and their citizens living in information societies.

The secrets for the Nordic countries' successes in cyberspace remind one another. For instance, "Sweden has in place a virtuous circle. A conducive environment, combined with the highest degree of readiness and widespread use of ubiquitous technologies, maximize the economic and social impacts of ICT, create new business opportunities, foster innovation, and contribute to reinforce a knowledge-based economy."[22] Finland's "level of readiness is first rate, thanks to its world-class educational system, relatively inexpensive technologies, and excellent infrastructure."[23] Furthermore, "Denmark posts some of the world's highest per capita figures in terms of Internet users, fixed and mobile broadband Internet subscribers, and PCs. The use of virtual social networks is pervasive, as reflected in Denmark's score (6.6 out of 7) and rank 2nd (behind Iceland) in the associated indicator."[24] Norway, again, excels in terms of individual usage as "some 90 percent of households are equipped with a computer and have access to the Internet. Overall, 93 percent of the population use the Internet on a regular basis (the second-highest percentage after Iceland)."[25]

The Nordic Cyber Security Levels

The Nordic countries strive for better cyber security through national policies. Most of them have cyber security goals incorporated in their overall strategic planning. However, most of the Nordic countries are still in the process of adopting a distinct cyber security strategy. Denmark lacks such a strategy. Sweden adopted a strategy for Internet security in 2006, but this document cannot be regarded as a full cyber security strategy for cyber is a wider concept than Internet security. Norway published a draft in 2010, and Finland did not adopt a cyber security strategy until early 2013. In fact, it was Estonia that became the first European country to publish a cyber security strategy. The document was published in 2008, following the severe cyber attacks Estonia suffered in 2007.[26]

[20] Ibid.
[21] Doutta & Bilbao-Osoriot, eds. (2012). p.xxiii & 3.
[22] Doutta & Bilbao-Osorio (2012), p.17.
[23] Doutta & Bilbao-Osorio (2012), p.17.
[24] Doutta & Bilbao-Osorio (2012), p.17.
[25] Doutta & Bilbao-Osorio (2012), p.17.
[26] Grauman (2012) p.57.

Despite the lack of distinct cyber security strategies, in worldwide comparison the efforts of the Nordic countries (regularly) result in high ratings in terms of cyber preparedness. The Graumans Cyber-security study of "The Vexed question of global rules", supported by the Security & Defence Agenda and McAfee, placed Finland, Israel and Sweden ahead of the United States in terms of cyber security.[27] The reasons behind this high rating can be found in the individual assessments:

Denmark's high rating, among other factors, is based on the country's CERT efforts – nationally, internationally and within the EU. Notably, Denmark also "has a contingency plan for cyber-incidents. It does not yet have a cyber-security strategy." [28] In addition, the "Danish military doctrine references cyberspace as a military battle space but does not provide details of concrete technical and operational capacity." [29]

Estonia was rated with four stars on a five star scale, like Denmark, due to its CERT efforts. "Estonia has a national CERT since 2006 (CERT-ee) and a cyber security strategy (since 2008). The country participates in informal CERT communities, and in the EGC Group of national CERTs. Estonia takes part in cyber-incident exercises."[30]

Finland has high ambitions in terms of cyber security with the goal to become the leading country in this area by 2016 [31]. Earlier Finland aimed to become a world leader in information security by 2015. In Grauman's study Finland reached four and a half stars out of the possible five thanks to the integration of cyber security efforts. "Finland's approach to cybersecurity has distributed the responsibility for cyber defence throughout the government and military. Finland considers that cyber security, in normal conditions, poses a greater threat to industry and business than to the military."[32] Finland's commitment to CERT was also noted in the study. "Finland has a national CERT (CERT-Fi), participates in informal CERT communities and is an active member of the European government CERTs Group (ECG). The country also engages in regular cyber-incident exercises in the public and private spheres."[33] Recently Finland has adopted a cyber security strategy, which could result in an even higher rating in a reassessment of the country's capabilities.

Norway began developing a cyber security strategy in 2009 and a proposal was published in 2010. Norway was not included in the Grauman study. However, a similar study that focused on the Military Doctrine, Organizations for Cyber Security and Cyber Warfare recognized that "Norway completed the drafting stage of the National Cyber Defence Strategy in 2010, and the legislative phase was to commence at the end of that year.[34] The Ministry of Defence will implement the Strategy. The Strategy proposes 22 measures to strengthen Norway's ability to prevent and manage cyber events".[35] The main objectives in the Norwegian cyberstrategy are to establish situational awareness and understanding of the cyber threat and to secure information and communication system, both civilian and

[27] Ibid.
[28] Ibid.
[29] Lewis & Timlin (2011), p.9.
[30] Grauman, (2012), p.58.
[31] Finland's Cyber Strategy, Government Resolution 24th of January 2013, http://www.defmin.fi/files/2346/Finland_s_Cyber_Security_Strategy.pdf.
[32] Lewis & Timlin (2011), p.11.
[33] Grauman (2012), p.61.
[34] http://www.regjeringen.no/nb/dep/fd/aktuelt/nyheter/2010/Horing-om-ny-cyberstrategi.html?id=599852
[35] Lewis & Timlin (2011), p.17–18.

military.[36] The National Security Authority (NSM) holds the overall responsibility for cyber security in Norway.[37] The Ministry of Defence is one of the driving forces in the efforts to develop a comprehensive strategy for cyber security. Recognizing the important role of cyber security for the military the Norwegian Cyber Force was officially established in September 2012 in Lillehammer and it holds well developed competence in the area.[38] The Ministry of Justice and Public security is in charge of the civilian part of the task.[39]

Sweden adopted a strategy for Internet security in 2006.[40] However, the document is not fully comparable with a cyber security strategy. The political structure in Sweden poses challenges to implementing a comprehensive cyber security strategy. The challenge is due to the governance structure of the authorities, which are basically autonomous even in crisis.

The National Post and Telecom Agency has a coordinating role with the right to issue cyber security related recommendations to other authorities.[41] The Swedish Civil Contingency Agency (MSB) was created to fill a support function for societal contingency planning. It also assumes a coordinating and advisory role over other authorities and the private sector in the field of information security.[42] MSB will work in close cooperation with the Swedish Armed Forces in order to analyze [and create] future systems to protect confidential information. In 2011, Sweden released a "National Response Plan for Serious IT incidents" which emphasized cooperative approaches with relevant industries and other agencies.[43]

Sweden was rated with four and a half stars in the Grauman study. "Sweden has a national CERT (CERT-se) that is a member of the EGC Group, and that takes part in informal CERT communities. It has a national cyber-security strategy, a national plan for cyber-incidents and organizes and participates in cyber-exercises." [44]

Cyber Security: Cooperation or Competition?

Security is needed in cyberspace like in any other space – on land, at sea, and in air. One of the challenges is to fulfill the requirements of cyber security in a world that has become increasingly hyper connected. Because "hyper connectivity is deeply redefining relationships between individuals, consumers and enterprises, [but also] citizens and governments", there is a need to cooperate across traditional borders. It has been assessed that our economies and societies are undergoing a fundamental transformation.[45] This transformation is so revolutionary that the Finnish Foreign Minister Erkki Tuomioja argues that "the classical approach to foreign policy and international relations, which has been dominating ever since the 1648 Treaty of Westphalia, is outdated and unworkable. Interdependence in things both good and bad, and whether we like the idea or not, is what governs international relations in today's globalized world. This applies not only to relations between states but

[36] Ibid.
[37] http://hvorhenderdet.nupi.no/Artikler/2010-2011/Nye-sikkerhetstrusler-cyberangrep/(part)/6
[38] http://forsvaret.no/om-forsvaret/organisasjon/felles/cyberforsvaret/Sider/cyberforsvaret.aspx
[39] http://www.regjeringen.no/pages/38169727/nasstratinfosikk2012.pdf
[40] http://www.pts.se/upload/documents/en/strategy_internet_security_2006_12_july_2006.pdf
[41] Ibid.
[42] http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Sweden.pdf
[43] Lewis & Timlin (2011), p.35.
[44] Grauman, (2012).
[45] Doutta & Bilbao-Osorio (2012), p.v.

also more generally. The concept of absolute sovereignty is a fiction that does not reflect reality anymore."[46]

In International Relations, the aforementioned perspective reminds the liberalist will to co-operate in order to live with and manage threats, including cyber threats. It depends on the "right attitude"; and the right attitude is about understanding the interdependences of the information age and openness to new possibilities, which may mean using social media in a new way. Increased collaboration, fueled by social media technology, links various actors in cyberspace and generates value for everyone, for instance, by improving cyber security. Cyber security is sometimes regarded as a challenge of securing sophisticated technology with the means of sophisticated technology. However, adopting this definition would disregard the human factor. Singer and Wright, for example, question the excessive use of technology and propose a pre-emptive banning of certain high-tech equipment and methods. This is to be done to meet ethical values and to prevent people from being hurt by malicious cyber attacks or unmanned weaponry, also known as drones.[47] To sum up, it is all about the human being and the ability to use technology for one's own advantage.

Therefore, we can also regard social media as "fundamentally a leadership and management challenge, not a technology implementation" for any social organization, whether it is a state, an NGO or the military. Bradley & McDonald argue that achieving mass collaboration provides organizations with "unique capabilities to create value for customers, employees, and stakeholders". This is a point of view that suits those who put cooperation first in their ideology and on their agenda, not competition and rivalry.[48]

It has been widely recognized that where there are "new opportunities, there are new challenges and risks in terms of individual rights and privacy, security, cybercrime, the flow of personal data, and access to information"[49]. The foundation of realism[50] states that there is a continuous struggle for power, control and influence; a competition or rivalry on who will lead and who will be lead. The realists assume that states are the key actors in international politics and that the inter-state relationships are at the core of international relations. Experts of realism acknowledge the continuing power of state as a major force shaping the international relations.

In contrast to classical realists, neo-realists such as Robert Keohane and Joseph Nye suggest that a concept of complex interdependence describes the world politics more accurately. From this perspective cyberspace is not a neutral environment where everybody can act like belonging to the same family. This brings us to perceive cyberspace as divided between the strong and the weak, the rich and the poor, the digital and the analog.

Whether we see activities in cyberspace through the eyes of realism or liberalism, we can argue that cyberspace is a space based on information technology. In addition, it is a space where states and individuals seek to promote their own interests in a social context. With

[46] Tuomioja, Erkki (2012).
[47] Singer & Wright (2013).
[48] Bradley & McDonald (2011). p.xiii.
[49] Doutta & Bilbao-Osorio (2012), p.v.
[50] There is not a realism of international relations. Basically, classical realism (e.g. E.H. Carr and Hans Morgenthau) has been kept apart from neo-realism (e.g. Joseph Nye and Kenneth Waltz). See more of International Relations Theory Booth & Smith (eds.), 1995.

regard to security, this means that non-neutral cyberspace needs different kind of security both in a technological and in a social sense.

Conclusion

All Nordic countries are defensive in the creation of cyber security policies. Therefore, it is a relevant question whether this is a good way to arrange cyber defence. According to Richard Clarke's[51] assessment on the best countries to attack and defend in cyberspace, North Korea is best equipped for cyber defence. This is a very paradoxical conclusion because North Korea is one of the least networked countries in the world, yet the best in cyber defence. Certainly, the weakness explains the strength. However, returning to the Stone Age is not an option. Thus, this paradox motivates the questions of how the Nordic countries should arrange their cyber defence, how the military forces should relate to cyberspace in general, and what role will they play in future wars.

Cyberwar, whether it is a real war or just hype, is a phenomenon that exists in war and peace – and in between these two. It appears in the discourses of both states and businesses, as well as of several other kinds of communities. This phenomenon, as evidenced by the articles in this book, is most likely too complex for the Nordic countries to deal with it on their own. This notion forces them to co-operate.

The level of co-operation, for the most part, depends on the political will since there is already potential and expertise available in these countries. Furthermore, cyberspace, cyber security and cyberwar are not clear concepts, nor is cyber defence. Especially, as cyberwar has been linked with war and the armed forces, even if otherwise cyber is not war and not owned by or on the responsibility of the armed forces. The entire concept of cyberwar is unclear, foggy and messy.

Undoubtedly, future wars will be messy[52]. In this respect, it does not matter whether these wars will be cyberwars or not. They will retain the same characteristics that wars have always had, but they will also have elements that the world has never seen before. Consequently, there is a need to question the concept of cyberwar, because only by questioning it we can estimate how serious cyberwar might become to modern societies.

Considering cyberwar a broad phenomenon, rather than a strict war, allows examining different perspectives rather than holding to only one clear-cut and tight definition. This grants room for Nordic co-operation in the area of cyber security. Following Heidegger allows assuming that observable events are enough to be a phenomenon, and cyberwar, to be comprehended, should be seen as the event of man. Therefore, the question is not whether cyberwar is about offense and/or defense. It is rather how to meet the phenomenon of "cyberwar" and how to endure problems that arise in the context of cyberspace when not necessarily defining them as a war. One of the most interesting concepts to explore in this context is that of cyber resilience, which is closely tied to the concept of cyber security and thus, to the phenomenon of "cyberwar".

[51] Clarke & Knake (2010).

[52] See more on messywars Huhtinen & Rantapelkonen (2008).

References

Bradley, Anthony & McDonald Mark (2011). The Social Organization. How to use social media top tap collective genius of your customers and employees. Harvard Business Review Press, USA.

Clarke, Richard A; Knake, Robert K. (2010). Cyber war. The Next Threat To National Security and What To Do About It. HarperCollins, New York.

Demchak, Chris (2010). Cybered Conflict vs. Cyber War. New Atlanticist, Policy and Analysis Blog. Available at http://www.acus.org/new_atlanticist/cybered-conflict-vs-cyber-war

Dempsey, Judy (2013). Cybersecurity: Munich finally takes notice. Feb 2, 2013. Available at http://carnegieeurope.eu/strategiceurope/?fa=50824

Doutta, Soumitra & Bilbao-Osorio, Beñat, eds. (2012). The Global Information Technology Report 2012. Living in a Hyperconnected World. World Economic Forum, April 2012, p.xxiii & 3. Available at http://reports.weforum.org/global-information-technology-2012/#=

European Union, (2011), Sweden Country report, ENISA, http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Sweden.pdf

Finnish Government, Finland's Cyber Strategy, Government Resolution 24th of January 2013, http://www.defmin.fi/files/2346/Finland_s_Cyber_Security_Strategy.pdf

Grauman, Brigid (2012), Cyber-security: The Vexed question of global rules. SDA (Security and Defence Agenda) & McAfee (An Intel Company), February 2012, p.79. Available at http://www.mcafee.com/us/resources/reports/rp-sda-cyber-security.pdf?cid=WBB048

Gray, Colin S. (2009). The 21st Century Security Environment and the Future of War. Parameters, Winter 2008–2009.

Heickerö, Roland (2013). The Dark Sides of the Internet. On Cyber Threats and Information Warfare. Frankfurt am Main: Peter Lang.

Heidegger, Martin (1977). The Question Concerning Technology, and other essays. New York: Harper & Row.

Huhtinen, Aki; Rantapelkonen, Jari (2008). Messywars. Finn Lectura, Helsinki.

Kaspersky Lab, (2013), Kaspersky Lab Identifies Operation "Red October," an Advanced Cyber-Espionage Campaign Targeting Diplomatic and Government Institutions Worldwide, http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_Operation_Red_October_an_Advanced_Cyber_Espionage_Campaign_Targeting_Diplomatic_and_Government_Institutions_Worldwide

Lewis & Timlin (2011). Cybersecurity and Cyber warfare. Preliminary Assessment of National Doctrine and Organization. Center for Strategic and International Studies.

Mcafee *Cyber-security (2012), The Vexed Question of Global Rules, available at* http://www.mcafee.com/us/resources/reports/rp-sda-cyber-security.pdf?cid=WBB048

Norwegian Government (2010), Horning om ny cyberstrategi, http://www.regjeringen.no/nb/dep/fd/aktuelt/nyheter/2010/Horing-om-ny-cyberstrategi.html?id=599852

Norwegian Government (2012), Nasjonal Strategi for infomasjonssikkerhet, http://www.regjeringen.no/pages/38169727/nasstratinfosikk2012.pdf

Norwegian Military (2013), Cyberforsvaret, http://forsvaret.no/om-forsvaret/organisasjon/felles/cyberforsvaret/Sider/cyberforsvaret.aspx (Last Read 30 Jan 2013)

Nupi (2011), Nye Sikkerhetstrusler: cyberangrep, http://hvorhenderdet.nupi.no/Artikler/2010–2011/Nye-sikkerhetstrusler-cyberangrep/(part)/6

Olson, Parmy (2012). We are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency.

Owens, William A., Dam, Kenneth W., & Lin, Herbert S (2009). Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities. Available at http://www.steptoe.com/assets/attachments/3785.pdf

Post och Telestyrelsen (2006), Strategy to improve Internet Security in Sweden, http://www.pts.se/upload/documents/en/strategy_internet_security_2006_12_july_2006.pdf

Rid, Thomas (2012). Think Again: Cyber war. Foreign Policy, 2. Aug 2012

Singer P. and Wright T. (2013) "An Obama Rule on New Rules of War", Brookings, http://www.brookings.edu/research/papers/2013/01/an-obama-doctrine-on-new-rules-of-war?cid=OtB_Inaugural_BB_News-Site_ad5&utm_source=Outbrain&utm_medium=TextLink&utm_term=News-Site&utm_content=ad5&utm_campaign=Outbrain-Inaugural-BBEU

Stiennon, Richard (2012). Is an International Cyber Regulatory Agency Needed? Forbes 22 Aug 2012, available at http://www.forbes.com/sites/richardstiennon/2012/08/22/is-an-international-cyber-regulatory-agency-needed/

STT (2012). Suomi matkalla kyberpuolustautumisen kärkivaltioksi. Available http://www.hs.fi/kotimaa/Suomi+matkalla+kyberpuolustautumisen+k%C3%A4rkivaltioksi/a1305593597540

Techeye.net (2013), Cyberwar is now Cleaner but far more Dangerous, http://news.techeye.net/security/cyber-war-is-now-cleaner-but-far-more-dangerous

Tuomioja, Erkki (2012). Speech by Mr. Erkki Tuomioja, Minister for Foreign Affairs, Finland, at the Armenian Diplomatic Academy, April 4th, 2012.

World Economic Forum (2012), The Global Information Technology Report, WEForum, http://reports.weforum.org/global-information-technology-2012/

Sovereignty in the Cyber Domain

Topi Tuukkanen

Abstract

The Westphalian state system is challenged by cyberspace, but it seems capable of adjusting to contemporary challenges. The central concept of the system, sovereignty, and its territorial manifestations need yet to be enforced in the cyber domain. NORDEFCO nations need to monitor the on-going development trends – ideally also to influence them. Nations are recommended to establish a multi-national cross-scientific research programme to consider the implications and challenges of cyberspace. The research programme is to take place in the scientific branches of international security studies, foreign and security policy as well as legal issues, and it should support the conceptual clarification of the role of the defence forces in cyber domain.

Keywords: Cyberspace, cyber domain, sovereignty, territoriality, jurisdiction, Westphalian state system

The Westphalian State System in Transformation

The contemporary international state system, the so-called Westphalian system, has evolved into its current form after the Thirty Years' War. The main concept to arise from the peace treaty of Westphalen in 1648 was the doctrine of sovereignty. It established the principles that govern anarchy inherent in international state-to-state relationships. However, developments in ubiquitous networking and events in cyberspace seem to challenge the Westphalian state system. Yet, do they do that? Is it possible for states to exercise their sovereignty and control in a borderless world?

The strengthening perception that cyberspace may pose threats at the national level implies that in the Westphalian system all states, in one way or another, will eventually initiate measures to control what they fear on Internet. If states cannot protect their economic base for wealth-creation, the capacity of a state will become questioned by those who control the resources under threat. This development is already underway.

States have been slow to respond to the predatory behaviour of malicious actors in cyberspace, thus neglecting their duty to reinforce their monopoly of violence over external threats facing their nations and harming their citizens. Even today, in many countries the development and the implementation of legal instruments and laws are more focused on internal symptoms than on external sources of the uncertainties.

Nevertheless, nations and states are already recognizing that cyber threats can become existential threats to the society in general and thereby to undermine the very purpose of the state. This can be concluded from the fact that many nations have already published or are just about to start their own work on national cyber security strategies. The establishment

of various national cyber coordination centres and/or military cyber commands, the re-arrangements of regulatory and CSIRT authorities, and the establishment of offensive cyber capabilities within military testify about the same development.

To sum up, it can be argued that the contemporary Westphalian system is changing and that the ability of the state to provide stability and security within its borders is seriously challenged by cyberspace – for the time being.

This article discusses some of the sovereignty issues in the cyber domain in layman's terms with the clarity needed for a non-expert. The article draws mainly from the body of writings of Wolff Heintschel von Heinegg (2012), but it includes inputs from renowned international legal scholars as referenced at the end of the article. Potential errors or misconceptions are solely those of the author.

Sovereignty

Krasner (2011) has conceptualized sovereignty in four different ways:
1. Domestic sovereignty; for example, organization of public authority
2. Interdependence sovereignty; for example, border control
3. International legal sovereignty; for example, mutual recognition of states
4. Westphalian sovereignty; that is, the exclusion of external authorities from domestic authorities

A number of other attributes and properties are required to properly characterize states in the international system. However, these are beyond the reach this article.

International legal scholars consider the concept of sovereignty to be one of the doctrinal issues challenged by the nature and the characteristics of cyberspace. Moreover, this challenge is seen as a difficult one because of the structure of Internet and the way in which the underlying protocols operate.

The concept of territorial sovereignty is addressed in conjunction with territorial jurisdiction in this article. However, sovereignty points to another concept as well, especially in the context of International Armed Conflict (IAC), namely to that of neutrality. The concept is also beyond the scope of this article, yet cyber neutrality is an area worth of further studies in itself.

The basic principle of territorial sovereignty declares that the state exercises full and exclusive authority over its territory.

1. The concept of sovereignty encompasses the notion that the "*State alone is entitled to exercise jurisdiction, especially subjecting objects and persons within its territory to domestic legislation*".
2. The concept of jurisdiction should be understood broadly as the "*state's lawful power to act and power to decide whether and, if so, how to act, whether by legislative, executive or judicial means*".

3. Territorial sovereignty also mandates the state to exercise control of access to and from its territory including all forms of communication. The methods and extent of such control are left to the state to decide.

The concept of territorial sovereignty shields the state from any form of interference by other states. However, the state has the "*obligation to protect the rights of other States, in particular their right to integrity and inviolability*". This leads to an essential foundational principle of international relations, that is, that other independent states respect the territorial sovereignty of a state.

The notion of state sovereignty also includes an additional dimension – that of sovereign immunity. As a practical example, the notion of sovereign immunity applies to a government (state) vessel in high seas. In times of international armed conflict, the principle of sovereign immunity is not applicable between the belligerent states.

Sovereignty is not only protective in nature. On the contrary, it also imposes some obligations. The foremost obligation arises from the definition itself – namely that a state is to respect the territorial sovereignty of other states (including political integrity). This obligation binds the activities of state organs. Furthermore, it was expanded in International Court of Justice (1949) Corfu case to an obligation of every state "*not to allow knowingly its territory to be used for acts contrary to the rights of other states*", that is, it leads to the **duty of prevention**. The applicability of the duty of prevention is contested by the question of whether the state needs to know, directly or indirectly, that hostile activities are conducted from its territory or not? It seems that most eminent legal scholars in the area are centering on the notion that the duty of prevention might be applicable even if the state is not aware of the hostile events. However, it has not been settled yet, partly due to the nature of routing on Internet, whether the duty of prevention is applicable in a case where data transits through a state, even if the transit state knows or should have known about the transit.

The events in Estonia and Syria in 2007, in Georgia 2008 and in Iran in 2010 demonstrate that hostile cyber activities are taking place in cyberspace, where the traditional law of armed conflict cannot be applied. These kinds of activities have been and continue to be a very handy strategy when states choose to exercise coercive diplomacy. The cyber option seems to be very attractive and less costly in comparison to the use of traditional military means.

Territoriality

It is an interesting note to a layman that border control, as implied above, is not merely an authorisation or permission for the state. Under customary international law, the state control of territory is closer to a requirement for the state to be regarded as a state at all.

According to Demchak and Dombrowski (2011) "*Today we are seeing the beginnings of the border-making attempts across the world's nations. From the Chinese intent to create their own controlled internal Internet, to increasingly controlled access to the Internet in less-democratic states, to the rise of Internet filters and rules in Western democracies, states are establishing the*

bounds of their sovereign control in the virtual world in the name of security and economic sustainability" (see also, for instance, Clean-IT project funded by the EU Commission).

Hare (2009) has analysed the national security concerns brought by the clandestine transnational actors in illegal drug trafficking. He postulates that state responses to drug trafficking show analogies with potential state security responses in cyberspace. None of the analysed six responses is adequate alone, and it can even be contested whether these six courses of action together will suffice. However, the observation that actions in other domains may bear resemblance to actions needed in cyberspace may prove to be a useful notion to further develop conceptual clarity needed for coherent cyber activities.

Expanding his analysis, Hare (2009) used the Interdependent Security Theory to suggest that borders are relevant components in the state-level responses to cyber security threats. Borders are important conceptual structures because they define technologically, procedurally but also psychologically the parts of cyberspace which are considered more or less secure – or insecure, depending on the viewpoint.

Conceptually, the establishment of borders in cyberspace make it more difficult, costlier and more time consuming to cause harm. Demchak and Dombrowski (2011) argue that the introduction of virtual borders is a part of an already established and evidenced natural process of states in adjusting the Westphalian system to the present day realities. In addition, they claim that virtual borders are technically possible, psychologically comfortable, and systematically and politically manageable. The so-called Stoltenberg Proposal for the Nordic CSIRT authorities' secure network or the Finnish Government Security Network Program can be seen as examples of the development towards this direction.

Franzese (2009) posits that sovereignty requires the state to be able to implement some measure of control over its cyberspace. Actually, he goes as far as to suggest that without the capability to monitor and control the borders in cyberspace, the concept of sovereignty in cyberspace is meaningless.

However, for those engaged in political science or international security studies it seems that further research is needed. Hare (2009) claims that improvements in a state's cyber security posture may provoke another state to follow suit, thus invoking what is known as the "security dilemma". He continues that it is of utmost importance that nations cooperate internationally in the implementation of security measures in cyberspace.

Cyberspace

There seems to be a growing number of international legal scholars who support the position that cyberspace is not a new "fifth domain" that would need new norms of international law. On the contrary, "*states seem to agree that customary international law is in principle applicable to cyberspace although there may be a need for consensual adaptation to the specific characteristics of cyberspace*".

Internet technologies offer anonymity and ubiquity, and the World-Wide-Web as an environment is an outcome of interconnected networks, telecommunication infrastructures, information systems and services. Therefore, it seems logical to consider cyberspace as "global commons" since cyberspace in its entirety is not subject to the sovereignty of a single state or a group of states. In the early 2000s, US Joint Chiefs of Staff (2012) defined cyberspace as "*a global domain within the information environment, whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit via interdependent and interconnected networks using information-communications technologies*".

The early confusion about the nature of cyberspace led to the misconception that cyberspace is "not a physical place". The reader may observe how the conceptual thinking has evolved by comparing the aforementioned definition with the definition of the term <cyberspace> developed jointly by the Russian and the US experts in Rauscher & Yaschenko (2011). According to this definition "*Cyberspace is an electronic medium through which information is created, transmitted, received, stored, processed and deleted*". There is no mentioning of domains, environment or unique characteristics!

So, even if cyberspace in some circumstances may be considered as "global commons", the already existing body of evidence of state practices points to the fact that the components of cyberspace are neither immune to state sovereignty nor to the exercise of jurisdiction.

A clear example of the states' exercise of jurisdiction is the criminalization of undesired (criminal) activities within cyberspace. Furthermore, states regulate legally, functionally and technically the operations of Internet service providers and the telecommunication infrastructure utilities. These activities highlight the notion that in order to exist, cyberspace must have physical artefacts, components, cables, devices, and protocols. The respective equipment is usually located within the territory of a state. It is owned either by government entities or by businesses. Therefore, the mere fact that a component has been connected to the World-Wide -Web, or Internet, is **not** to be considered a waiver from the state jurisdiction. Of course, the technologies, protocols, and properties pose challenges to the actual exercise of state sovereignty but that does not mean that the state could not overcome the challenges.

Herrera (2008) argues that there is nothing inherent about technologies. They are human creations and as such subject to conscious and unconscious shaping by social actors and institutions. Thus "*global digital networks have the features they do, of placelessness, anonymity and ubiquity, because of politics, not in spite of them*". He thereof foresees potential for two parallel developments that are of interest to us:

– firstly, the re-territorialization of Internet which would mean placing controls to cyberspace that allow greater control by territorial entities and
– secondly, the de-territorialization of national security as an adaptation of states to digital networks – states reconfigure their practices but not along the territorial lines.

Under the political pressure these two distinct, opposing realms are moving closer to one another.

Actually, scholars seem to agree that, unless limited by specific rules of international law (for example, human rights), the cyber infrastructure located and the cyber activities taking place in the territory of a state are subject to almost unlimited prescriptive and enforcement measures by the respective state. Again, it needs to bear in mind that such activities may give rise to security or power-security dilemma, or even contest the general perception of security as felt by the citizens. The latter has been described in more detail by Buzan (1991).

However, the traditional interpretations of customary international law may not be applicable as such. In view of the novel character of technologies, scholars and governments are yet unsure whether the traditional interpretation of customary international law would yield desired results. Therefore, we can expect that scholars and governments continue their efforts to establish stabilised and shared interpretations of international legal norms and the respective behaviour in cyberspace.

As Franzese (2009) points out in his comprehensive treatment of sovereignty in cyberspace, states:

1. should acknowledge that the portion of cyberspace under their jurisdiction is a sovereign domain
2. must recognize that exercising state sovereignty in this cyberspace is in the national strategic interest
3. need to manage civilian expectations of the state sovereignty in cyberspace
4. should develop the technical capability to exert their sovereignty in cyberspace.

Furthermore, Franzese (2009) notes that in order for states to exert sovereignty in cyberspace, an international regime (with specific rules and procedures regulating state activity) needs to be formulated, either by practise or by treaties, as it has happened in the sea, air and space domains. The customary nature of international legal norms means that we shall see a number of cyber events that sometimes lead to a new interpretation and sometimes not. As noted by Brown (2011), an example of this chain of events and missed opportunities was Stuxnet; the Iranian regime has not yet taken any action to raise that event for the consideration of the international legal community.

The principle of territorial sovereignty in cyberspace stems from the notion that the cyber infrastructure is located on the national land territory, on the territorial waters, in the national airspace, in a vessel or aircraft registered or flagged to the state in question. However, there are a number of well-established exceptions to sovereignty, for example, the immunity of diplomatic correspondence or the right to innocent passage.

On the other hand, while cyber infrastructure falls under the jurisdiction and the sovereignty of a state, the same principle simultaneously protects states from the interference of other states. This protection is not limited to the use of force by another state, but it covers a broad range of other, potentially hostile activities that are attributable to the other state and that fall under the notion of the violation of sovereignty. Moreover, in this case of "protection", it is irrelevant whether the infrastructure is owned by governmental agencies or by private industries.

Nonetheless, the reader should be cautioned: legal scholars seem to consider that in order for a cyber attack to amount to a violation of sovereignty the consequences, material destruction, and the loss of life need to be substantial. Thus, it seems that there is more work to be done to address how the international community is going to respond to hostile cyber actions that cause no or minimal damage and thus do not qualify as a violation of sovereignty. So far most nations have decided to pursue such events through domestic cybercrime legislation and international cybercrime cooperation – often with dismal results.

Within international customary law, cyber espionage is an interesting case. International customary law does not in any way limit or prohibit espionage, which leaves that area of operations completely unregulated. In general, espionage does not cause destruction or deaths that would justify the notion of a violation of sovereignty. On the other hand, depending on the details of attribution, the mere fact that foreign state organs have intruded into the cyber infrastructure of another state can be considered as an exercise of jurisdiction on a foreign territory. Such an act always constitutes a violation of the principle of sovereignty.

The concepts and legal notions described above mainly relate to activities that are attributable to a foreign state whereas the international legal framework addresses the state to state relationships. However, in view of the architecture and the characteristics of cyberspace, it would be virtually impossible to attribute a cyber attack to an actor – at least when the attack is underway. Attribution would be enormously challenging even with a broad international support and cooperation, and it would take a long time – rendering the results inconclusive, insufficient, or otherwise useless for a timely response in political/strategic sphere. However, tracing down the event may bring out some new observations – at least with regard to the modus operandi.

To summarize, the principle of state sovereignty and the right of a state to exercise territorial jurisdiction apply to the cyber infrastructure within the territory concerned. Moreover, states do have control over cyber activities that are:
– initiated by individuals present in that territory or
– taking place within the territory or
– producing harmful effects on the said territory

These legal constructs translate to similar concepts in the technological domain:
– cyber event originating internally but terminating externally
– cyber event originating externally but terminating internally
– cyber event transiting

For our consideration cyber events originating and terminating internally are domestic issues to be addressed by national criminal legislation.

Implications for the Nordic Defence Cooperation

Most forms of commerce, social constructs and citizens thrive on order and regularity. It is the responsibility of the state to establish such conditions. So far, cyberspace has undermined that responsibility but states are catching up – or are they?

In the first chapter we recognised that cyberspace is challenging the contemporary Westphalian state system but that this system is capable of adjusting and changing. The question is how do we participate and direct that change? Enforcing the Westphalian state system in cyberspace needs to pay due respect to the civil liberties and 'individual information self-determination' that are seen as core values to be protected, yet these core values need balancing with national security.

In the second chapter we learned about the concept of sovereignty and that international customary legal system is expanding the scope of the "Duty of Prevention". However, this development is still debatable. Moreover, as many Nordic nations are telegeographically positioned to be transit states, it is important to note that international legal norms regarding transit are still under development. Although not directly addressed in the article, emerging transit norms are of utmost importance to those Nordic nations that plan to opt for non-alignment or neutrality in any future conflict or crisis.

In the third chapter we examined the concept of territoriality which led us to consider borders in cyberspace. Borders are important conceptual structures as they define technologically and procedurally, but also psychologically, which parts of cyberspace are secure and which are not. We also noted that these kinds of developments are already underway in NORDEFCO nations.

In the fourth chapter we learned that the notion of cyberspace as a global common is rapidly falling out of fashion. Moreover, the trends of re-territorialization of Internet and de-territorialization of national security need to be monitored. State recognition and implementation of its sovereignty in cyberspace are not yet conceptually clear in NORDEFCO nations and they need to be supported by research and cross-scientific studies.

Furthermore, we learned that although cyber espionage is not regulated by international legal regime, cyber intrusions may in certain circumstances amount to a violation of sovereignty. Considered generally as peaceful and with defensive postures, NORDFECO nations would be well advised to control their government organs' cyber activities abroad closely.

From these considerations, the final recommendation for NORDEFCO can be concluded. It is to consider the establishment of a multi-national cross-scientific research programme to consider the implications and challenges that stem from cyberspace and that bear relevance to politics, international security studies, national security, foreign and security policy, role of the defence forces in the cyber domain, as well as domestic and international legal developments.

References

Biersteker, T. (2002). State, Sovereignty and Territory, in Carlsnaes, W. et al.(eds.): Handbook of International Relations, Sage

Brown, G. (2011). Why Iran did not admit Stuxnet was an attack? Joint Forces Quarterly 2011(63):70.

Buzan, B. (1991). People, States & Fear: An agenda for international security studies in the post-cold war era. 2nd ed. Hemel Hempstead, UK: Harvester Whatseaf; 1991.

Demchak, C & Dombrowski, P. (2011) Rise of a Cybered Westphalian Age. Strategic Studies Quarterly 2011

Franzese, P. (2009). Sovereignty in Cyberspace: Can it exist? The Air Force Law Review, Vol 64

Hare, F. (200). Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security. In: Czosseck C, Geers K, editors. The Virtual Battlefield: perspectives on Cyber Warfare: IOS Press

Heintschel von Heinegg, W. (2012). Legal Implications of Territorial Sovereignty in Cyberspace. In 4th International Conference on Cyber Conflict; Tallinn, Estonia: CCDCOE

Herrera, G. (2008). Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space. In: Dunn M, Krishna-Hensel S, Mauer V, editors. Power and Security in the Information Age: Investigating the Role of the State in Cyberspace. London, Ashgate

International Court of Justice (1949). Corfu Channel Case 9th April 1949.

Jensen, E. (2011). Sovereignty and Neutrality in Cyber Conflict. Fordham International Law journal, Vol. 815

Joint Chiefs of Staff. (2011). Department of Defence Dictionary of Military and Associated Terms. Joint Pub 1–02

Korns, S. & Kastenberg, J. (2009) Georgia's Cyber Left Hook. Parameters – US Army War College, Vol. 60

Krasner, S. (2011). Problematic sovereignty: contested rules and political possibilities, Columbia University Press

Liaropoulos, A. (2011). Power and Security in Cyberspace: implications for the Westphalian state system. In Panorama of Global Security Environment, Bratislava: Centre for European and North American Affairs

Rauscher, K. & Yaschenko, V. (eds). (2011). Russia-US Bilateral on Cybersecurity: Critical Terminology Foundations. New York, USA: EastWest Institute

Cyberspace, the Role of State, and Goal of Digital Finland

Jari Rantapelkonen & Saara Jantunen

Abstract

This article aims to engage the Finnish cyber narrative from the perspective of original idea of cyberspace. It discusses the representation and the narratives of future Finland, as presented by the Finnish authorities through the "Digital Finland" document written in 2010. Digital Finland is a report on future prospects of the Finnish society by the Ministry of Transport and Communications. It proposes three alternative government programs for managing Finnish communication services and labels them as "progressive", "dynamic" and "decisive". These proposals make rhetorical claims and narrative assumptions about what is noteworthy in cyberspace, providing empirical data for analysis. The results show that the alternative programs are not only positive metanarratives of imagined future, but arbitrary and vague, political description. The "decisive" program is listed as the best choice for the future of Finland, but it remains political, and not necessary reflecting the original idea of the nature of Internet. In terms of content, Digital Finland fails to recognize the interrelationship between information technology and social life as complex questions of life in information society, and at cyberspace.

Keywords: Digital Finland, cyberspace, Finnish government, Ministry of Transport and Communications

Introduction

Finland is a keen supporter and an avid actor in developing the Nordic welfare model. The model itself is, according to the latest program of the Finnish Government, based on a high employment rate, competitive economy, and accessible services and care for all[1]. This is what is considered the best social system -- a model that combines social cohesion and competitiveness. The Finnish government is willing to take a determined approach to improving the basic structures of the welfare society.

Information and technology are defining the structures of welfare society. Finland has been a pioneer in the field of broadband and mobile telephone technology, which have been the key innovations of the information society for the everyday lives of Finns. In 2003, there were some 300 000 broadband connections in Finland, compared to 2,4 million households. In 2006 the number of broadband connections had increased to 1,4 million, meaning 50 per cent of households were connected. According to the Global Information Technology reports, in 2006–2007 Finland ranked number four in the world in the networked readiness index. In 2007–2008, Finland fell to the sixth position, staying there until 2009–2010. The latest Global Information Technology Report 2010–2011 confirms that the leadership of the

[1] Finnish Government (2011).

Nordic countries and the Asian Tiger economies in adapting and implementing information and communication technology advances both growth and development.

Nature of Cyberspace

Globalization has challenged the nation state. Creation of cyberspace meant a new kind of political, economic, military, legal, and ethical discussion of the role of nation state. The nature of cyberspace has many features that are very complex, as no-one can define what actually cyberspace is, who are present, and what is the size of cyberspace. Therefore, it is very difficult to deal for anyone wishing to control digital globalization.

Cyberspace, for example, Internet is not only physical entity, but a giant network which interconnects vast amount of users, groups, societies, states and non-governmental institutions. Most of the users exchanging information by using computers do not notice, or even care of national borders that cannot be seen in cyberspace. Users are not even are aware of national norms while having communication throughout the world. One of the features of what cyberspace is doing to our presence is "the extreme reduction of distances". In this sense users are everywhere from homes and shopping malls to work places and courthouses, and ubiquitous presence in seconds is a fact. With ubiquity, Paul Virilio argues that interactivity and immediacy are key features of cybernetic environment, which takes to the conclusion as speed belongs to the core functions of cyberspace that "it is impossible to differentiate between information and disinformation".[2]

Cyberspace is not only "heaven", but expanding exponentially going through its own inflationary period from secret military research circuit to digital domain playing a greater role in more and more people's lives. Cyberspace is a place to socialize and play through chat rooms, newsgroups, IRC channels, and other social media, online conferences, and forums. "In a very profound sense this digital space is "beyond" the space that physics describes, for the cyber-realm is not made up of physical particles and forces, but of bits and bytes." Weinberg is clear that "These packets of data are the ontological foundation of cyberspace". This is the reason why cyberspace is not subject to laws of physics.[3]

In some profound way, cyberspace is another place where our "locations" can no longer be fixed purely in physical space. Just "where" we are when we enter cyberspace is a question yet to be answered. This must be a challenge for the government, police and military whether man is in physical or data space. However, cyberspace is much more to be stressed, "[t]he primary use of cyberspace is not for information-gathering but for social interaction and communication – and increasingly also for interactive entertainment, including creating fantasy worlds. Digital domain may take us back to Gibson's Neuromancer where Gibson imagined "that when his "console cowboys" donned their cyberspace helmets, they were projected by the power of computer-gathered three-dimensional illusionism into a virtual data landscape.[4]

[2] Virilio, Paul (2000), p.13.
[3] Wertheim, Margaret (1999), p.228–229.
[4] Wertheim (1999), p.230–233.

Regulating and controlling cyberspace is challenging for any entity, corporate, to government. Cyberspace exists and functions as a result of millions of users of computers and networks decided to use a common data transfer protocol. There is no centralized storage location, control point, or communication channel for cyberspace. This is the reason why "it would be impossible for any single entity to regulate the information conveyed on the Internet."[5]

Government: Finland a Leading Country in the Development of Cyber Security

The Finnish government has recognized that the reliability of information networks is vital to the operation of modern information societies. The newly elected government in 2011 has declared cyber issues as a matter of "security and defence policy". Preparing a cyber strategy for the national information security is an important objective. Also important is to actively participate in international cooperation in the information security field. "Finland's goal is to become a leading country in the development of cyber security."[6]

Actually the aim of "leading light" was already mentioned in the Government Resolution on National Information Security Strategy called "Everyday security in the information society - a matter of skills, not of luck." The strategy was adopted by the Finnish Government on the 4th of December 2008. The aim of the National Information Security Strategy is to make everyday life in the information society safe and secure for everyone in Finland. Strategy defines everyone as individuals and businesses, administrative authorities, and all other actors in society. Strategy defines the vision for Finland as "people and businesses will be able to trust that their information is secure when it is processed in information and communications networks and related services." According to the National Information Security Strategy "by 2015 Finland will be the leading country in the world in terms of information security."

The National Information Security Strategy focuses on three priority areas: 1) Basic skills in the ubiquitous information society, 2) Information risk management and process reliability, and 3) Competitiveness and international network cooperation." The term 'information security' mentioned in the 2008 Government document has been replaced by 'cyber security' in 2011. One may ask whether these are synonymous concepts or what the difference is, if the aim is has remained the same.

Defining the "transport and communication policy", the Finnish government sets a role for the information and communication technology: "The importance of information and communications technology for the improvement of growth and productivity is decisive." The government refers to the economic growth and the productivity of industry arguing that clear goals will be set for improved productivity. More particularly, the government declares what kind of aims Finland has with communications technology: "The provision and use of high-speed broadband connections will be promoted to make Finland the leading European country in terms of broadband access. The introduction of high-speed broadband connections will be promoted throughout the country and the expansion of the

[5] ACLU (1996).
[6] Finnish Government (2011).

freely-available wireless network will be accelerated." One of the projects to enhance this is *Broadband for All by 2015*.[7]

For citizens, the government promises that "[a]ll citizens will be guaranteed barrier-free participation in the information society and the digital world regardless of their income level, health, financial status or place of residence." The government clearly is against digital exclusion and would like to see all citizens to be members of digital Finland. "The goal is to make digital data materials managed by the public sector available to citizens, companies, enterprises and organisations, authorities, and for research and education purposes in an easily reusable format via information networks", announces the Finnish government[8].

From Connectedness to Productivity and Well-being – Digital Finland

Digital Finland is a 2010 report on future prospects by the Ministry of Transport and Communications. It discusses themes relating to the Finnish society that require guidelines in the Government Program in 2011–2015. The report puts forward three "suggestive" government programs, labeled as "Progressive Finland", "Dynamic Finland" and "Decisive Finland". The report states that it does not take a stance for any of the suggestive programs, but that "based on them, it is also possible to put together different entities with varying emphasis relating to transport and communications policies"[9].

"Progressive Finland" is the most moderate option of the suggested three. The aim is to increase the productivity of businesses and the public administration. The general aim is to advance democracy and Finland's competitiveness. [10]

"Dynamic Finland" aims to promote digital Finland as part of digital Europe. It, as well, aims to improve productivity and therefore the well-being of the citizens.[11]

"Decisive Finland" is the most radical with its aims. According to this program alternative, Finland is aiming for a remarkable competitive edge in international markets and economy[12].

In addition to the theme of productivity, *Digital Finland* discusses the improvement of networks. The basic idea is that the Ministry of Transport and Communications seeks to promote an efficiently functioning society and national well-being by making sure that people and businesses have access to high-quality, safe and reasonably priced communication networks. This is ensured by competition between communications companies.

[7] Finnish Government (2011).
[8] Finnish Government (2011).
[9] LVM (2010), p.3.
[10] LVM (2010), p.3.
[11] LVM (2010), p.3.
[12] LVM (2010), p.3.

Analysis and Discussion

This analysis focuses on three sections of the report, which discuss the digitalization process from the perspective of information networks. First, the references to the interdependence of productivity, communication and connectedness are discussed. The second part of the analysis focuses on the security discussion of the report. Third, the analysis is concluded by discussing the labels of each program: What makes the progressive program progressive, or the decisive program decisive?

a) Who is who in Digital Finland?

This section discusses the first part of the *Digital Finland* report, which focuses on productivity.

In the report, the three program alternatives are presented side by side. Each program alternative first introduces the aims and a plan of their actualization. The following table (Table 1) lists these elements: first the aim and then the actors that are mentioned, and finally the proposed actions. The chart below presents the contents of the three program alternatives:

Aims of Progressive Finland ("Edistyvä Suomi")	Improving the productivity of the private and public sector, improve public services and welfare, and advance democracy and competitiveness through information society policies.
Actors	● Government administration ● Businesses ● Information Society Council ● Universities, research organizations
Actions	● The development of information society is continued by coordinating it nationally and by participating in international cooperation ● Information society work is coordinated between government and business representatives in the information society council ● Maintain and observe national information society strategy work ● Found a secretariat for the matters of information society ● The "smart strategies" of all branches of administration are composed in the supervision of ministries and in the coordination of information society council ● Public sector information administration is developed ● Universities and research organizations are encouraged to participate in information society research and development work
Aims of Active Finland ("Aktiivinen Suomi")	The Government advances digital Finland as part of digital Europe. The productivity of businesses and the public sector are being improved. Welfare, democracy and competitiveness are being improved.
Actors	● Ministries ● Cabinet committees ● Government

Actions	• The management and improvement of digital progress are included in the tasks of the ministries • A cabinet committee is founded to incorporate the work of different branches of administration • In the supervision of the cabinet committee, the ministries compose their "smart strategies" that are based on the needs of the branch user • The government decides on the Digital Finland operational programme which is used to improve sustainable productivity in the society • Public information reserves are used in the development of electrical services • The public sector information administration is developed and electrical public services advanced through corporate guidance • Steer public research funding to the basic social research of digital society
Aims of Decisive Finland ("Rohkea Suomi")	The government determinedly advances digital Finland as part of digital Europe. Through the use of information - and communications as central strategies, the productivity of businesses, the services and welfare of the citizens are being improved, and democracy is advanced. The aim is to achieve a significant, international competitive advantage.
Actors	• Ministries • Cabinet committee
Actions	• A cabinet committee is founded. In its supervision a Digital Finland operational program, which takes into account the needs of the users in each branch, and the qualitatively and quantitatively measurable smart strategies. The smart strategies must work towards the improvement of sustainable productivity. • The Cabinet committee prepares the procedures of the ministries in the matters of communication policy, the advancement of information and communication, communication technology, innovations, the copyrights of digital society, privacy, electrical trade, and other matters of advancing digital Finland. • The public information reserves are widely opened for the development of electrical services • The Cabinet Committee also supervises the public sector information administration, which is developed through strong corporate guidance in the government and municipal information administration. • Steer significant amounts of public research funding to the basic social research of digital society

Table 1: Aims, Actors and Action descriptions in Digital Finland

The observations that can be drawn from the section of the report are that

1. *Progressive Finland* is characterized by ambiguous action descriptions, such as "improve sustainable productivity". *Active Finland* and *Decisive Finland* present more descriptive actions and responsibilities; *Decisive Finland* is the most detailed about who does what. All programs are described in the passive form, which makes them more or less ambiguous.
2. The program titled as *Progressive Finland* brings up cooperation that would involve both, the businesses and the government administration. The role of government increases in *Active Finland,* and even more so in *Decisive Finland.*
3. Competitive and productivity are assumed to rise according to the increase of government control.
4. Only *Decisive Finland* explicitly states its aim ("competitive advantage").

Even though the authors of *Digital Finland* claim they do not favor any single option of the three, the ambiguity of *Progressive Finland* and to a degree of *Active Finland* makes them the less attractive options, whereas *Decisive Finland* is presented as the most comprehensive and thorough option of the three.

b) Digital Security

In the section on digital security, the government is presented as the only actor. All three programs mention cooperation between government and the private sector, but again the trend is that *Decisive Finland* is the most comprehensive and concrete version of the three options. The role of the state and government is, again, most prominent in Decisive Finland, although strongly present in *Active Finland* as well. These characteristics are presented below (Table 2):

	Action	**Target**	**Actor**
Progressive Finland	Develop	communication and information networks and the security of their control in cooperation between government and businesses	(passive form)
	Fulfill	national and international information security responsibilities	(passive form)
	Ensure	the undisrupted operationality of the information society	(passive form)
	Decentralize	procurement of information networks and services	Government
	Take into account	extreme weather conditions	(passive form)
Active Finland	Strengthen	the supervision of telecommunication businesses	(passive form)
	Deploy	cooperation in the supervision and management of central infrastructure	(passive form)
	Minimize	risk concentration of communication and information systems	(passive form)
	Promote	competition	(passive form)
	Keep	the critical systems of government networks separated from public networks	(passive form)
	Observe	ownership of critical communication networks	(passive form)
	Obtain	the most critical parts of the networks into the ownership and control of the government	(passive form)
	Improve	government information security through corporate management	(passive form)
	Ensure	communication services in case of the increase of extreme weather conditions	(passive form)
	Legislate	about critical problems of information and communication networks.	(passive form)
	Ensure	services through management	(passive form)
	Incorporate	the cooperation of government officials and businesses in the supervision of the Ministry of Communications	(passive form)

Decisive Finland	Secure	the undisrupted operability and usability of digital services and communication networks	(passive form)
	Strengthen	the cooperation between government officials and businesses	(passive form)
	Ensure through legislation	that businesses produce necessary services to respond to all national and international threats and infrastructure disruptions	(passive form)
	Invests heavily	in the development of the safe communication network it manages	Government
	Develop	the formation of situation awareness and, in case of a serious disruption or state of emergency, a comprehensive cooperation network for surveillance and control	(passive form)
	Ensure	communication services in case of the increase of extreme weather conditions	(passive form)
	Improve	the operability of communication networks	(passive form)
	Create	a legislative foundation for the joint use and construction of traffic routes and communication and electricity connections	(passive form)

Table 2: Actors and Actions in Digital Finland

As demonstrated in Table 2, the level of abstraction is higher in *Decisive Finland* due to the combination of abstract verbs and abstract objects. Passive constructions are used throughout all three program alternatives.

c) Progressive, Active or Decisive – but What Would Make Finland so?

The prologue of the report describes the programs as moderate policy-making with the emphasis on already existing assets (*Progressive Finland*), as "active" policy making with new points of emphasis (*Active Finland*) and as heavily prioritizing policy-making (*Decisive Finland*). The authors also estimate that the policy introduced in *Progressive Finland* would not be likely to demand more resources, whereas *Decisive Finland* would. In other words, the amount of government control correlates positively with the need for funding, whereas public/private cooperation is seen as moderate and low cost.

The cyber domain seems to be more or less understood as a technical tool for improving the economy a society where productivity is a high aim. The vision is that a global, computerized, networked economy is the one Finland is aspiring to. Some experts have even argued that profits for the Finnish society can be in the billions. Without question, *Digital Finland* sees information and communications technology in a positive light, whereas dreams of "ubiquitous", "fast" networks and "connectivity" are a path to a better economy and life.

On the other hand, the document sees the information society vulnerable for the interferences and interruptions.

Conclusion

Digital Finland is a grand narrative of imagined cyberspace that unveils the best future without negative aspects of cyberspace. The future, according to the narrative, will be better, if government is put in the front lines of cyber security development and responsibility.

Cyberspace, according to the "decisive" program (which is obviously the preferred option), is very much an environment or instrument necessary to achieve the best productivity and economic growth for Finland. *Digital Finland* contains the idea of a close connection between the pursuit of economic efficiency and digitality.

However, *Digital Finland*'s metanarrative does not discuss the consequences of possible fragmentation of other narratives that have been present in the shadows of globalization. *Digital Finland* is actually silent about the other options for leading development of cyber security.

Digital Finland is also silent about disappearance of the Subject. Therefore the future *Digital Finland* proposes is very much about emphasizing both, power and politics, where digitality is the part of technology that actually is a mode of revealing what Heidegger has written about technology. The future of *Digital Finland* reveals only one form of a computer culture. This takes us back to Sherry Turkle's findings on cyber cultures and how "[i]n the 1970s through the mid-1980s, the ideology that there was only one right way to "do" computers nearly masked the diversity of styles in the computer culture. In those days top-down thinkers didn't simply share a style; they constituted an epistemological elite"[13]. Turkle proposes that in this postmodern age of cyberspace, the unity of self (or organization) is an old-fashioned fiction. Cyberspace provides the opportunity for splitting the self into a radical multiplicity, as Wertheim writes about Turkles message[14].

The nature of technology includes the paradox that claims "to bring the future under the rule of instrumentality, while it both largely devoid of historical awareness and the primary source of the disruptions that will falsify any expectations of the future"[15]. *Digital Finland,* in the name of productivity and efficiency, denies how the past and future of technology are disruptive. The "decisive" program contains the idea of the inseparability of power, desire, and truth. Future digital Finland with the "decisive" narrative is actually the desired way of doing "business", but also a desired life, which cannot be an explicitly presented as a utopian dream, nor an implicit presentation of the invisible, such as Neuromancer's cyberspace: "A consensual hallucination experienced daily by billions…"[16] Denying the disruptiveness of the future is typical for high-tech narratives, and in that sense *Digital Finland* is not different from any other plans of technology for the future cyberspace.

Politics is a struggle between narratives. *Digital Finland* recognizes the production of services, such as broadband for every Finn and online services as its outcome. This 'revolutionizes' and turns human life into digital life in order to create economic productivity. This is the key to better life in cyberspace in digital Finland. It should be noticed that the concept of

[13] Turkle (1995), p.54.
[14] Wertheim (1999), p.247.
[15] Ross (1990), p.261.
[16] Gibson (1984), p.51.

cyber or digitality are not clearly defined - or, in fact, defined at all. This is what should make us approach *Digital Finland* critically. According to the report, the citizens of digital Finland should trust the government that determines the policy on communication and its organization, but also decides to introduce the society to the 'improved cyber life'. Digital Finland does not discuss how cyberspace or "the digital environment is foremost a culture of rapid changes and adaptability: it is a cultural phenomenon driven by social adaptations of technological innovations, and thus it calls for a dual inquiry into its inner mechanisms and structures"[17].

This takes us to think about the competitive edge, "customer is always right", and whether this approach suits the aims of digital Finland. However, in the future, life will be experienced through the computers and lived at the screens - which is already very much the state of hybrid virtual life of many who reshape cyberspace. This is no longer a future challenge for the political narratives -- it is our present. Customers are different. One may ask why Finland wants to be number one in cyber security, is the vision and strategy appropriate for the postmodern age, and do people or customers living cyberlife want to be at top. One can only wonder, and ask should and when a government's traditional conception of power in the age of postmodern cyberlife should change to respond reality of cyberspace.

References

ACLU (1996). 1996 WL 311865 (E.D.PA.), American Civil Liberties Union et al., v. Janet Reno, Attorney General of the United States, American Library Association, Inc., et al., v. United States Department of Justice et al., Nos. CIV. A. 96-963, CIV. A. 96-1458, United States District Court, E.D. Pennsylvania, June 11, 1996.

Dutta, Soumitra; Mia, Irene (2011). The Global Information Technology Report 2010-2011, Transformations 2.0. World Economic Forum, Geneva.

Finnish Government (2011). Programme of the Finnish Government, 22 June 2011. Available at
http://www.valtioneuvosto.fi/hallitus/hallitusohjelma/pdf332889/220611hallitusohjelma_en.pdf

Doueihi, Milad (2011). Digital Cultures. Harvard University Press, Cambridge, Massachusetts, and London, England.

Gibson, William (1984). Neuromancer. Ace books, New York.

LVM (2011). "Suomi tietoturvan suunnannäyttäjäksi. Suomalaisen tietoturvaosaamisen levittäminen ja aktiivinen osallistuminen standardien kansainväliseen kehittämistyöhön", The Ministry of Transport and Communications. Julkaisuja-sarja 17 / 2011. Available at http://www.lvm.fi/c/document_library/get_file?folderId=1551284&name=DLFE-11972.pdf&title=Julkaisuja%2017–2011

[17] Doueihi (2011), p.xvii.

LVM (2010). “Digitaalinen Suomi, uusi liikennepolitiikka. Liikenne- ja viestintäministerön tulevaisuuskatsaus puolueille 10.9.2010”, The Ministry of Transport and Communication. Julkaisuja-sarja 33 / 2010. Available at http://www.lvm.fi/c/document_library/get_file?folderId=964900&name=DLFE-10937.pdf&title=Julkaisuja%2033-2010%20LVM%20Tulevaisuuskatsaus%2010092010

Ross, Stephen David (1990). “Power, Discourse, and Technology: The Presence of the Future”. In Shapiro, Gary (ed.). 1990. After the Future. Postmodern Times and Places. State University of New York, Albany, NY, pp.255–272.

Turkle, Sherry (1997). Life on the Screen: Identity in the Age of the Internet. Simon & Schuster.

Virilio, Paul (2000). The Information Bomb. Translated by Chris Turner. Verso, London.

Exercising Power in Social Media

Margarita Jaitner

Abstract

Social media has become an influential tool for exercising power. The world has testified a number of situations in which it has served as an important element in organizing and developing a socio-political protest movement.

The article shows how social media can be used as a tool in political struggle. It scrutinises the question in the light of the electoral protests during the 2011/2012 elections in Russia. The article focuses on government's capabilities to counter opposition that grows within social media. It introduces a number of possible counteractions by basing on Nye's theory on hard and soft power. However, it is also suggests that the possible ways to counteract a certain protest movement are dependent on the situation in which they arise. In practical application this means that each case has to be addressed on the basis of its specifics.

Keywords: Social media, social networks, Twitter, "Twitter revolution", social unrest, Russian elections 2011–2012, Hard and Soft Power

> *"Today, no governement in no country can ignore the existence of a vast network of communications that emerge, develop and live, whether the governments like or not. We need to create the right legal framwork for the development of social networks, but we cannot blok them."*
>
> *Dimitry Medvedev*

Social Media in the Time of Unrest

Undeniably, social media has a great impact on many people's lives. It is used for both personal networking and entertainment. However, social media is more than just networking – it enables people to express themselves and speak for their cause in many different ways. One can post a blog entry, upload a picture on Tumblr or share an article on Pinterest. Some of these actions are only meant for the users' friends and are of a strictly private content. Others are designed to advertise a product or a service. Those belonging to a third variety are to disseminate information to a wider audience in order to promote a cause.

The role of social media in organizing protest movements and/or disseminating information on socio-political issues has, undoubtedly, attracted the attention of both journalists and scientists. The significance of technologies, such as text messages and social media tools, has been widely discussed in the context of the events that are now known as the Arab Spring. In early 2011, social media, Twitter, and text messages in particular, were widely used to disseminate information on people's dissatisfaction with their governments and to

coordinate protests in Algeria, Bahrain, Egypt, Morocco, Tunisia and Yemen. Journalists quickly coined the term "twitter revolution", and scholars have also noted the significance of the information technology for political movements.[1]

For the sake of completeness, it should be mentioned that the events of the Arab Spring were not the first case of intense utilization of social media in political struggle. The Zapatista movement demonstrated already in the mid 1990's that social media can be used as a tool for exercising power.[2] In Iran, social media was (unsuccessfully) utilized during the election protests in 2009.[3] Nevertheless, some scholars argue that social media does not change the nature of political struggle but merely facilitates it, and that it does not necessarily have an impact on the outcome.[4]

The utilization of social media in political struggle is not limited to authoritarian states. On the 6th of August 2011, a peaceful protest turned violent in one of the northern districts of London, the UK. The country's major cities faced widespread riots, arson, and looting in the following days. Rioters organized mass gatherings via various social media platforms and the BlackBerry Messenger service.[5] However, there was a flip side to the use of social media. Investigators screened social media platforms during and after the riots in order to identify persons who were taking part in hooliganism.[6] The overall impact of social media was deemed to be of such significance that the British Prime Minister David Cameron suggested that it should be possible to limit access to certain social media, if it was suspected that those were used for plotting criminal actions.[7]

In Russia, the Duma elections held in December 2011 spawned numerous protests after the allegations of falsification by the then Prime Minister Vladimir Putin's party, Yedinaya Rossiya, were spread online. Social media outlets, such as YouTube and blogs, were used to spread claims that supported the allegations of rigged elections. Widespread use of Internet platforms, such as Twitter, Live Journal, YouTube and other social networking sites, has kept the protesters' outrage fresh in the people's minds for months.

Social Media as a Tool in Political Struggle

Internet provides for a number of activities that can be connected with the promotion of a movement. As identified by Arquilla and Ronfeldt[8] these are:

- Collection of information
- Publication of own information
- Dialogue and debate concerning the issue

[1] Hounshell (2011)

[2] Zapatista (the Zapatista National Liberation Army, EZLN) movement, active 1994–1998; Arquilla; Ronfeldt (2001) pp. 171–172; Arquilla; Ronfeldt (2001) pp. 178ff By the use of social media they managed to get their agenda through not only to their followers, but also to international fora and could thereby place pressure on the Mexican government.

[3] Zuckerman (2011)

[4] Zuckerman (2011)

[5] Dodd; Davies (2011); Halliday (2011a)

[6] Halliday (2011b)

[7] Guynn (2011)
"[…] whether it would be right to stop people communicating via these websites and services when we know they are plotting violence, disorder and criminality[…]"; BBC (2011a)

[8] Arquilla; Ronfeldt (2001) p. 242–250

- Coordination of action with like-minded people and groups
- Lobbying decision makers by creating a discourse in the population

Subsequently, it is suggested in this article that it is possible to react to any of these activities in a particular and suitable way. The government might see it necessary to interfere with some cases in order to calm down or even to suppress the movement. However, not all responses are feasible due to various socio-political considerations such as international political pressure, the country's economic situation or technological abilities, or protesters' anger.

One of the most basic governmental responses is to block off the access to Internet entirely or just to certain sites. However, as the experience has shown in the case of Egypt[9], this way of handling the problem is highly problematic in a number of areas. For one, Mubarak's blocking off the access to social media resulted in harsh criticism by the international community. This put a strain on the external cooperation with his government and weakened the regime.[10] For another, the blockage resulted in financial loss for Egypt's economy. This has been likely to result in decreasing internal support for Mubarak.[11] In addition, blocking off the access to social media is not a simple task to perform due to the nature of technology. There are various means to work around a blockage – such as the use of proxy servers as it was done in Tunisia.[12] A total shut down of Internet access can also result in difficulties in investigating the origin of the unrest and/or the possible lines of support from unfriendly nations or organizations.

Depending on the individual situation the government might limit its online actions to observing the growing unrest and to collecting information on those who incite the unrest and activities. This would allow the government to react with meaningful real-life measures. For example, in the case of the riots in 2011 in the UK, findings in social media were used to identify and to prosecute those who committed crimes during the riots. The government may also use data collected in social media in its attempts to estimate the number or the type of security personnel required to handle a mass gathering, or whether there is a need to protect a certain object.

In this article it is suggested that the government has more options to react to an unrest growing within social media than it has been publicly discussed in the context of the aforementioned cases. The very essence of social media offers a broad spectrum of conceivable methods to interfere with a movement growing within it.

Particularly, exercising the power of attraction within social networks seems logical. Nevertheless, is it possible to achieve immediate results by interfering in social media in any other way than by shutting down the access?

[9] Obama (2011)
[10] BBC (2011b)
[11] Zuckerman (2011)
[12] Zuckerman (2011)

Exercising Power through Social Media

In the global information age, the ability to utilize soft power is becoming a necessity.[13] Although the concept of soft power as a contrast to hard power has been continuously developed by Nye and other scholars of international relations, and although it enjoys great popularity in this field, it can also be applied in domestic policy.[14] Even states regarded as coercive apply soft power in their internal politics. The Communist Party of China, for example, explores the effects of the utilization of soft power in China's domestic governance, and claims to be applying it successfully.[15]

The interconnectedness of social media makes it easy to promote different causes with a variety of requirements for participation. Sites like www.causes.com suggest that everyone can change the world right from the comfort of his or her home. Slacktivism[16] and clicktivism are terms that are used to describe the low-input type of activism within social media, sometimes in a derogatory way. However, there is reason to believe that even this type of low-commitment, low-risk and low-cost activism within social media can influence the political discourse.[17] We can thus ascribe social media to certain means of power.

In order to be able to apply the theory of hard and soft power on events and action in social media, it is necessary to create a framework for classifying actions as a means of hard or soft power.

In international relations, the utmost exercise of hard power is often exemplified by military action against the subject of power. A parallel to this in the world of social media would be a complete denial of access to a platform. This can be done in a variety of ways in and outside Internet.

On the other hand, the means of soft power may seem more diffuse. They include any action that aims for co-option by the subjects of power. An appealing online self-presentation that does not include any elements of coercion or induction, and is regarded as worth of being shared by online users, is an example of a successful use of soft power in social media.

The transition from hard to soft power is almost seamless. Therefore, the used means are often classified as elements of "rather hard than soft power" or vice versa – instead of being labeled as elements of either hard or soft power. This implies that in terms of the use of social media the amount of hard and soft power can vary depending on how and what type of media is being used, or in which combinations. Moreover, it also makes a difference who is using social media and for what purposes. A framework for classification of cyber activity in terms of hard and soft power is suggested in Chart 1.

[13] Nye (2008)
[14] Zhang, Jiang (2010)
[15] Zhang, Jiang (2010)
[16] Oxford Dictionaries (2012)
[17] Rotman et al. (2011); Lindquist (2011)

Chart 1. Exercising of power in cyberspace

Scope and Limitations

Non-state actors are increasingly using social media to organize and coordinate activities. Therefore, a need arises to find practical solutions that enable the state or its sympathizers to counter these activities. Methods of counteraction can be seen as an exercise of power and hence they can be classified with the help of Nye's theory of hard and soft power.[18] The aim in this article is to provide an overview of the actions performed by opposition and to scrutinize how those were countered by the legal constitution and its sympathizers. In addition, the latter forms of action will be classified according to their scale of hard and soft power.

The article focuses on the time period between the 4th of December 2011, when the legislative (Duma) elections were held, and the 10th of May 2012, that is, the day after the annual large scale parade which is held in honor of the veterans of the Great Patriotic War and the Victory Day. The reasoning behind the choice of this particular end date was a desire to see whether the oppositional activity would continue with the same intensity on this important holiday.

The article scrutinizes the behavior of political actors, and their sympathizers, in a few social media platforms, namely Twitter, the Russian Live Journal blogs (known as Zhivoy Zhurnal, Живой Журнал or ЖЖ), Facebook and VKontakte (ВКонтакте, a Russian-language web platform similar to Facebook). Russian-language Internet is, of course, not limited to the aforementioned platforms, but these have been deemed most relevant for this article due to their high popularity in Russia[19]. This limitation means, however, that an extremely popular platform "Odnoklassniki" (Одноклассники, Classmates)[20] was omitted. The platform was omitted because it appears to be "out of the loop" of the otherwise interlinked political debate within social media.

As it has been mentioned, the focus of this article is on Russian-language Internet, RuNet, as Russians themselves call it. Due to the language barrier and its specific cultural context, RuNet remains relatively isolated from the rest of Internet.[21] For that reason, the assumption

[18] Nye (2004)
[19] Lonkila (2012)
[20] Lonkila (2012)
[21] Lonkila (2012)

is that even if an actor from abroad chooses to post something on RuNet, the message is aimed at the Russian society.

After years of state controlled press during the communist rule and the "half-freedom of speech" of the Putin era[22], there is little trust among the Russian population on media outlets such as TV or news papers. People have resorted to discussing politics in private and to expressing themselves in a humoristic way. Therefore, social media in Russia, and in other countries that experienced a prolonged period of regime-controlled media, has the potential to reach a different status and to fill a different function than in countries in which conventional media is regarded as a fairly credible source of information.

The article does not research political protests on Internet but is delimited to social media. Despite this limitation, it is important to understand that these platforms do not exist in a vacuum but live off the interconnectedness with the rest of Internet. In practice this means that social media is used to popularize information found elsewhere online. Articles, opinions, videos and pictures gain popularity by being posted, re-posted and judged in social media and thus become parts of it. For this reason, the article will include elements found outside social media – even if only to observe the significance of these elements in social media. Furthermore, it is important to examine the events taking place off-line due to the extreme inter-linkage between the on-line and the off-line worlds. Off-line events trigger on-line events, and vice versa. For this reason, the article will touch upon events outside Internet, although they are not its subject. The key is to understand how these events are relevant to the context of social media and, at the same time, to delimit the focus of the analysis to effects within social media. Applying the principle of denial of access to Internet or to particular parts of it means acting both in and outside Internet.

In many cases the government is opposed by a number of different ideologies and political opinions rather than a single, more or less cohesive group with a highly aligned agenda. For the purpose of this research there is no need to differentiate between these groups. Throughout the article the term "opposition" will be used to refer to any group that is opposing Yedinaya Rossiya. Furthermore, any action that interferes with oppositional operations will be classified as a "countermeasure" if any other actor, including a pro-Yedinaya Rossiya movement, can adopt this action for its own purposes.

Data used in this research includes postings on various social media sites, as well as articles and news found on various online outlets. This type of material is usually very problematic from an academic point of view. The same goes for the statements that are found on official Russian outlets, such as the state TV. Nonetheless, unreliability is not relevant for this article because of the way the data is utilized. When something is posted online, it creates a discourse and influences the public opinion. No official statement to correct the "untruth" will return the public opinion into what it was before the untruth was disseminated.

When applying this principle, the question is not what happened in reality but whether a piece of information was posted online and whether it has promoted a discourse. This means that data is not used to document events that are described in data but rather to observe the reaction it creates.

[22] Lonkila (2012)

Elections, Protests and Social Media

The Russian legislative elections (Выборы в Государственную думу) were held on the 4th of December 2011. There were seven parties registered for the elections, even if the opposition expected the then-ruling party, United Russia (Единая Россия), to win the elections by using dishonest methods. The opposition also voiced its mistrust.

In the evening of the 4th of December, activists considered the election process flawed and gathered together to demand the election results to be annulled. Many demonstrations and "meetings" (митинги) were held during the following weeks. The activity culminated in protests in many Russian cities and even abroad on the 10th of December. The march on Bolotnaya Square in Moscow was said to be one of the largest in the past decade in Russia. During the demonstrations activists from various parties formed an ad-hoc opposition with a common enemy, Yedinaya Rossiya, and a common symbol, a white ribbon. Nevertheless, each party also continued arguing for its own cause.

The Russian police, who were ordered to Moscow on the 6th of December, and the pro-Putin activists, Nashi (Наши), who organized demonstrations in favor of Yedinaya Rossiya, countered the "meetings". Arrests were made in many cases. Amongst others, one of the opposition's frontmen, Alexey Navalny (Yabloko), was taken into custody on various occasions. Another large-scale demonstration was held on the 24th of December, and even during the following months people gathered to show their lack of trust on Yedinaya Rossiya and on the elections.

Putin's candidature in the 2012 presidential elections was loudly disputed by the opposition. Following from the debacle about falsifications in the Duma elections some precautions were taken by the elections committee. The previously used solid urns were replaced by transparent ones and webcams were installed into the country's polling stations. These webcams were live streaming during the elections and could be watched on www.webvybory2012.ru[23]. Vladimir Putin won 63.60 % of the votes in the first round and hence won the election.

The committee's measures to raise trust on the procedure did not hinder the opposition from gathering for new demonstrations. The largest "meetings" were held on the 5th and the 10th of March. Again, numerous arrests were made on several occasions.
According to the official statements security agencies would only interfere with demonstrations if they turned violent or would otherwise break the law. Several allegedly not state-preapproved demonstrations were stopped by the special police forces (OMON).

The opposition began planning the Million's March (Марш Миллионов), a large scale demonstration, shortly after the official results were released. On the 6th of May, a day before Vladimir Putin's third inauguration, the demonstration took place in Moscow. During the demonstration different sources claimed that one or several people had died in the masses. Later it turned out that only one blogger had died following from a fall from a fire escape while trying to photograph the march. The security agencies were still claimed to be more brutal this time than during the previous months' demonstrations, and many arrests were

[23] After the elections, the videos were archived and they are accessible via the State and Municipal Services website http://epgu.gosuslugi.ru/pgu/service/-10000000413_418.html

made. The demonstration continued until late night. On the following day, the opposition gathered once again on Manezhnaya Square, Kitay-Gorod (Китай–Город) where the protesters stayed through the night and continued demonstrating the rest of the time period covered in this article.

Microblogs – Twitter

Opposition and the supporters of Yedinaya Rossiya campaigned and organized their protests[24] via Twitter and other online platforms while the traditional media[25] chose to focus on other news and barely mentioned the protests.[26] Interestingly, the online news outlet Utro (Утро, Morning) was quick in calling the previous days' events a "try to start a twitter revolution" on the 5th of December.[27] During the first demonstrations the derogatory term for the opposition, "little net hamsters" (сетевые хомячки), was coined and used as a hashtag on Twitter.[28]

Shortly thereafter, pro-Kremlin and completely non-related messages started to show up in the Twitter feed. These were using the same hashtags as the opposition, particularly #триумфальная (#triumphalnaya, Triumphalnaya square in Moscow), and quickly multiplied into a vast amount of messages which complicated the coordination of the protests. Cyber security experts had also identified an unusual and sudden rise in new Twitter account registrations, and connected these accounts with the messages that used the opposition's hashtags. A number of accounts had been identified as bots[29] and they were blacklisted.[30]

Whether a user account is used by a bot or not is, in many cases, easy to identify even by non-experts. Typically bots post new tweets much more frequently than a regular user. Some bots post several different or similar tweets per minute, something a human user would not be able to do – no matter how fast he or she could type. Other bots are seemingly human with a slower pace of posting.

Two types of bot accounts can be identified. The first type uses accounts that were newly registered for the bot, while the second type uses accounts that were registered by regular users. The latter can be identified by the pattern of their historical activity. The history of these accounts typically includes a number of private non-bot-related tweets followed by inactivity. The most recent tweets, again, can be attributed to bot activity.

As mentioned earlier, there were several types of information that could have been disseminated by bots. For one, a number of pro-Kremlin or contra-opposition tweets were to be observed. These included pro-Kremlin information or derogatory speech directed at the opposition. Other bots posted completely non-related tweets including links to different products. These can be compared with conventional SPAM that many users receive to their

[24] Nummelin (2011)
[25] Allegedly state-controlled official media outlets such as TV, radio, printed press.
[26] TT via Dagens Nyheter(2011)
[27] Gasparov (2011)
[28] Keen (2011)
[29] Goncharov (2011): Listing of Twitter bots recognized in December 2011.
[30] Rusecurity (2011), Goncharov (2011)

e-mail addresses. Since spamming is against the terms of usage, bot accounts are regularly identified and blocked by Twitter. However, it is only a matter of time when new bots become active.

Some human-only contra-activity could also be identified. In these cases, groups of users, who can be assumed to be human, tried to create another trending topic on Twitter. This topic would then compete with the hashtags used by the opposition.

An interesting contra-activity pattern could be observed between the 6th and the 9th of May. Very little contra-opposition activity took place during the first two days – with the exception of non-related hashtags that briefly peaked in trends. A non-related tag #Мяу (a cat's meow) was allegedly brought up by the pro-Yedinaya Rossiya movement. The picture changed radically in the afternoon of the 8th when Twitter was swamped by contra-opposition tweets using the opposition's hashtags and thus making the coordination of the opposition difficult. This continued on the next day with Victory Day topics trending.

Social Networking Sites – Facebook, VKontakte

A number of oppositional and pro-Yedinaya Rossiya groups were created on social networking sites Facebook and VKontakte before, during, and after the elections.[31] Alexey Navalny's group, RosPil (РосПил), soon became one of the most popular groups with over 140 000 members. Alexey Navalny also maintained a Facebook page, which, nevertheless, did not reach the popularity of RosPil. According to various sources the Russian Security Service, FSB (ФСБ), contacted the head of VKontakte Pavel Durov in the week after the elections asking him to take down RosPil. Pavel Durov declined to do so.[32]

These groups were created to discuss the events, disseminate information about the upcoming events and, as in the case of RosPil, act as a continuous campaigning platform. Many comments and entries included pictures hosted on sites like Twitpic and videos hosted on content sites such as YouTube. Many event pages that were created for the upcoming demonstrations ranged from zero to over 20 000 users planning to attend. Some of the event pages were later re-used for the following demonstrations and no longer hold the original description. However, during the research long lists of comments that pointed toward preparations for the demonstrations were found.

A closer look at the online opposition groups and events reveals a set of problems with the planning and promotion of demonstrations via these platforms. In order to gain popularity these groups and events were made open and free to join by anyone, which resulted in a strange pattern of participation. The event "Белая площадь" (Belaya Square in Moscow), for example, had over 3 700 members signed up for the demonstration, 505 who replied they would "maybe" attend and over 3 000 others who were invited. Amongst the attendees were a remarkably high number of accounts that had little or no ties to Russia or to Russian politics. A number of these accounts seem to have been abandoned by their original user and hijacked by bots. This irregularity had also been noted by the opposition and resulted in

[31] de Calbonnel (2011), Portalinski (2011)
[32] Forbes (2011), Soldatov (2011)

further discussion about the trustworthiness of both the pro-Kremlin and the oppositional movements.

The groups were occasionally joined by non-supporters eager to either discuss or to disseminate propaganda. Despite the non-supporters who can be referred to as "bots" there was no evidence of automated or coordinated behavior of this type. The term bot refers in this case to the lack of independent thinking. The regular members would more commonly refer to the non-supporters as "trolls", meaning provocateurs.

Blogs – Live Journal

Blogs were widely used both to create and to maintain a political discourse. They were also used as a platform to disseminate YouTube video links to alleged cases of electoral fraud. Blogs were the platform to share political opinions, news or rumors, as well as pictures taken during different actions and demonstrations. On several occasions, the blogs of the opposition were "trolled" by what were said to be pro-Kremlin activists. In some cases the events were similar to those on Twitter. Many previously inactive users would post more or less generic pro-Kremlin comments drowning the oppositional conversation out.[33] Several times these comments included vulgar language and insults towards the owner of the blog. Amongst the opposition these are now known as "Едроботы" (Yedroboty), an acronym for Yedinaya Rossiya's bots.

Members of the opposition have tried to follow up and analyze the occurrence of bots on Live Journal. What they came across, as Eduard Kot stated on his popular blog "edvvvard", was an ad for a freelance assignment looking for five people who would post 70 comments per day by using 50 different user accounts on assigned blogs for a salary of 12 000 RUB ($ 389) per month. Eduard Kot then claimed to have traced the origins of the ad back to the supporters of Yedinaya Rossiya. These findings triggered a further discussion about Yedinaya Rossiya's and Nashi's integrity. Some discussion regarding automated versus manual spamming of blogs was to be observed. Nonetheless, no evidence was found which would have supported a distinction between manual and automated spamming.

The popular blogging platform Live Journal suffered several so called DDoS attacks during the researched period. This resulted in service outages in the second week of December.[34]

Content Communities – YouTube

Accusations of electoral fraud were backed up by a vast amount of videos posted on YouTube from different polling stations across the country. Some of these were amateur recordings with the help of Smartphone; others were semi-professionally or professionally created videos by independent web-TV studios such as nk-tv.

[33] Elder (2011)
[34] Etling (2011)

Another group of videos and pictures posted on content communities were documentations of demonstrations and meetings. In many cases they aimed to document the behavior of security personnel. Several times videos and pictures were posted together with links to Facebook or VKontakte groups or blogs and hence they contributed to the interlinkage of social media.

Live streaming platforms, particularly ustream.tv, are a noteworthy subgroup of content communities. These sites provide a possibility to upload video content on Internet while creating it, for example, with a Smartphone camera. This feature makes live streaming platforms similar to live transmission on TV.

Surprisingly, no reference to political vlogs, video blogs, was found, albeit vlogging has found its way to the Russian online society. Other content sites were mainly used to support activity on particular social media platforms by providing content to blogs, social network groups and tweets.

Events outside Social Media

The following events occurred outside social media. Nevertheless, they were part of the discourse in blogs and social network groups and, therefore, they were deemed relevant for this article.

On the 4th of December 2011 websites of the radio station Ekho Moskvy (Эхо Москвы, Moscow's Echo), news outlets Kommersant (Коммерсантъ), slon.ru, Bolshoi Gorod (Большой Город, Big City) and The New Times were subject to a DDoS attack which resulted in their temporary unavailability. Website of the civilian association to protect Russian electoral rights, Golos, and its project "Map of Fraud" (Карта Нарушений) suffered the same fate.[35]

On the 6th of May Kommersant, Ekho Moskvy, slon.ru became once again victims of a DDoS attack together with the web TV station Dozhd (Дождь, rain.tv)[36]. On the 9th of May the streaming service ustream reported to be under an attack which seemed to target the account reggamortis1, a user known to stream protest videos.[37]

DDoS attacks were not the only hacker activities during the period covered in this article. A group which calls itself Anonymous Op_Russia claimed to have hacked a number of e-mail accounts that belonged to the activists of Nashi, and published these e-mail conversations. The leaked e-mails contained information on the planning of paid bot-like attacks on popular oppositional blogs as well as on paying news outlets for publishing pro-government articles.[38] Anonymous claimed via Twitter that it had also conducted a number of other attacks. Most recent of these were the attacks against kremlin.ru and other government websites in the last week of the conducted research.[39]

[35] BBC (2011c); Newsru.com (2011); Etling (2011)
[36] Gazeta (2012); Securitylab (2012)
[37] Taylor (2012a)
[38] Taylor (2012b); Elder (2012)
[39] EHN (2012); DI (2012) ; Infosecurity Magazine (2012)

A number of tools to support protesters were introduced in the wake of the mass protests. The site Philanthropy, for example, published a selection of resources such as phone numbers of lawyers who volunteered to help protesters in case of arrest, as well as a number of links to groups of civil assistance. For instance, the site helpwall.info "Стена помощи на митингах" provides a platform for organizing acute help via Twitter. By using the hashtag #help495 on Twitter or via text message protesters can, among other things, notify the public about their arrest or get in contact with a lawyer.

Action and Counteraction in Social Media

A number of different types of activity within social media were identified in the course of the research. The majority of online activity consisted of planning real life activities, promoting one's cause through blog entries, discussions in various groups, pictures and videos of events, and propaganda. In many cases entries aimed to defame one's antagonists. Another identified element was spamming which was done both manually and automatically. A large amount of unwanted entries interfered with groups' abilities to converse and plan events. Making social media unavailable by attacking websites technically lies outside the domain of social media. However, it has a significant impact on the use of social media and it is hence relevant for this article.

The collected data shows plenty of online activity that was directly or indirectly connected to the protest. Much of the activity can easily be ascribed to either side of the conflict. The origin of the rest of the activities is more ambiguous. Even if there are technical means to trace a piece of information – such as a blog entry, a comment, or a picture – back to its source, these means are often unavailable to users or even to researchers. This makes it difficult, if not impossible, for the researcher to verify pieces of information posted online. However, those who the information is primarily aimed at, in this case the Russian population, face similar difficulties. This obstacle to determining the truth of information found online is exacerbated by the longstanding attitude, held by much of Russian populace, of mistrust on the government and official news outlets.

Fortunately, neither the truthful origin of a piece of information or activity, nor the validity of the information is necessary for this research. It is more important to consider the perception of information or activity amongst the Russian population. As noted earlier this research focuses on activities that hinder the opposition from gaining influence. Therefore, the first step is to extract such activities from the pool of activities in social media.

Social media related activities that complicate the opposition's operations can be summarized as follows.

Countermeasure 1: Shutting down or limiting access
Shutting down or limiting access to the opposition's tools of communication and coordination within social media by attacking the media. This was demonstrated earlier in the article with the example of a successful DDoS attack against Live Journal. The countermeasure can lead to significant monetary losses.

Countermeasure 2: Shutting down elements within social media
Targeting certain elements within social media, for instance, a particular account or a group. This was demonstrated with the example of the alleged request to shut down RosPil on VKontakte. Unlike the aforementioned total shut down, this countermeasure presumably aims at splitting a homogeneous oppositional group that has become "too big" in the eyes of its antagonists. The method includes an element of threat thereby demonstrating one's power over an entity within the seemingly uncontrolled Internet.

Countermeasure 3: Attacking media outlets
Attacking other oppositional or seemingly neutral media is, similarly to the previously mentioned targeting of oppositional groups, a demonstration of power. When conducted against commercial entities, it can lead to a significant loss of income. This is likely to weaken and demoralize their financial stakeholders.

Countermeasure 4: Automated spamming of the Twitter feed
During ongoing demonstrations the automated spamming of the Twitter feed by using the topics and hashtags utilized by the members of the protest. This is often done in order to drown out information that is relevant to an ad-hoc organization. In these cases the opposition has no chance to fight the spamming process manually. It will have to resort to the use of other means, for example, a different hashtag.

Countermeasure 5: Spamming the Twitter feed manually
This can be done, for example, during ongoing demonstrations. The countermeasure is deemed different from automated spamming simply because an automated bot can generate new tweets at a much faster pace, and it is hence easy to identify as a bot. On the other hand, in manually conducted spamming activities human beings compete with human beings. The success largely depends on the number of people in the group and their level of motivation. This type of activity demonstrates commitment to a cause rather than willingness to use "brute force".

Human counteraction can also amend information, not only drown out the relevant messages. For example, it is possible to post misleading information on further demonstration plans in order to split up groups on the streets.

Countermeasure 6: Trending other topics
Popularizing other hashtags and topics than the ones used by the opposition on Twitter – as it was done in the case of the #Мяу (Meow) hashtag. The activity is similar to the manual spamming of the Twitter feed because it also aims at the demoralization of the opposition by showing their "unpopularity".

Countermeasure 7: Organized spamming of blogs
Organized spamming of blogs with unrelated or hateful comments and thus, drowning out the discussion – as it has been done to Alexey Navalny's blog on several occasions. The activity aims at disturbing the discussion. In the research, there was not enough evidence to conclude that automated spamming of media other than Twitter occurred, even though it is technically possible. Thus, no distinction between manually and automatically conducted spamming is being made at this point.

Countermeasure 8: Defame the opposition with facts
Using the gathered information to defame the opposition, for example, by pointing out that a large amount of people, who agreed to take part in the demonstrations, does not have any connections to Russia.

Countermeasure 9: Defame the opposition with forged information
Forging "facts" that defame the opposition and spreading them online. This can be exemplified with the case of the Facebook event "Белая площадь" in which the high number of participants was composed of persons with no obvious ties to Russia. Since there is no way to know who added these persons to the event, there are two possible explanations. Members of the opposition might have added them in order to create the illusion of massive support. Alternatively, those who aim at defaming the opposition might have added these participants only to accuse the opposition of "playing dirty" or exaggerating their popularity.

Countermeasure 10: Discussion
Partaking in discussion in the opposition's groups or blogs, as it was observed to have happened on various social media platforms, aims at changing the members' opinions and/or demoralizing the opposition.

Countermeasure 11: Blogs, groups etc.
Maintaining own presence within social media and lobbying for one's own cause.

The Means of Power

Because there is no definitive method to measure the "softness" or "hardness" of power – as such ranking procedure is highly subjective – the following results are merely a suggestion. By the application of a different approach some of the countermeasures could be deemed either harder or softer. It is thus suggested that the main indicator of the hardness of power is the amount of coercion that is included in the measure.

Countermeasures 1 and 2 are clearly examples of the exercise of very hard power; they are demonstrations of the uttermost coercion in cyberspace. Countermeasure 3 attacks a third party and aims at harming the opposition indirectly. This means that the opposition could continue operating. Therefore, this countermeasure is ranked slightly softer. However, the financial aspect discussed earlier puts this method clearly within the realm of very hard power.

Countermeasure 4 can actively interfere with the opposition's activities and is thus deemed an exercise of hard power. The interference is nearly physical and it includes a fairly high degree of coercion.

Countermeasures 5 and 6 are comprised of both hard and soft power. Depending on how these methods are used they may be classified as slightly harder or softer. The methods employ both coercion by interference and attraction by demonstrating human commitment.

Countermeasure 7 is similar to the countermeasure 4. However, it is not directed at the opposition's operations in the same way and is thus deemed softer than the countermeasure 4. As stated earlier, blogs are not used to disseminate real-time information but are rather platforms for a political discourse. Thus, only the opposition's discussion becomes disturbed, not its operations.

Countermeasures 8 and 9 are very similar in their effects. In many cases it is hard for an outsider to say which one is which. These actions aim at defaming the opposition. At the same time, they offer the public a trustworthy alternative to the opposition. The latter aspect places these countermeasures within the realm of soft power. However, the element of attack against the opposition adds coerciveness to them.

Countermeasures 10 and 11 are also very similar and are by definition means of soft power. These categories represent the softest power that can be exercised within social media as they do not seek to coerce.

How to Exercise Power in Social Media

"Shaping public opinion becomes even more important where authoritarian governments have been replaced by new democracies. "
Joseph S. Nye Jr. [40]

This article has revealed a number of methods that were used in Russia to counter the opposition's operation and coordination within social media. The countermeasures were ranked along the continuum of power from soft to hard depending on the amount of coercion they employed.

Shutting down the access to Internet or to certain parts of it, as well as pressuring the owners of social media platforms to delete oppositional groups, were the methods of the uttermost hardest power that were identified in the course of the research. The use of these tools, however, is likely to result in strong reactions inside the country as well as from the international community. Exercise of power in this way conflicts with the Western ideas of freedom and democracy.

Automated spamming of Twitter feed is a method that applies much less hard power than the aforementioned two methods. This method is very effective in disrupting ad hoc organizations. However, it does not entail much soft power either, because it is an inconvenience for the Twitter user. In addition, automation can be easily identified.

A number of methods utilize a combination of hard and soft power. Depending on how the methods are used either hard or soft power prevails. These methods are, first, manual spamming or trending of unrelated topics or contrary opinions on Twitter and, second, manual spamming of blogs and other social media platforms. They can be regarded as fairly effective, because they efficiently disrupt oppositional discussion or even ad hoc organization, and because they at the same time demonstrate the unpopularity of oppositional action.

[40] Nye (2004) p.6

Defaming the opposition with facts or with forged information and posting pro-government information in discussions and on blogs are classified as uses of soft power. As it is typical to the means of soft power, these methods are not immediately effective. They have no power to disrupt the oppositional discourse but they can amend it in the long run. These methods rarely have immediate results. Therefore, their success can only be verified or disproved after they have been applied for a longer period of time.

The proposed ranking of measures, in a range from hard to soft, is summarized and visualized in the chart 3. Some of the measures are granted a range rather than a point in the chart – as the research suggested. This ranking, however, is not absolute. Depending on the individual situation countermeasures can be either "harder" or "softer".

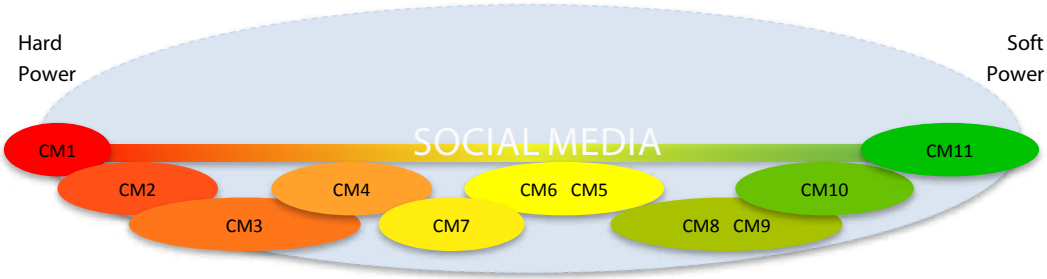


Chart 3. Countermeasures in terms of hard and soft power

Conclusion

The research has resulted in a set of methods that can be used to oppose a movement growing within social media. The classification of the means provides an estimate of the reactions that different actions might trigger. Knowing what can be done also raises awareness amongst those who take part in a movement or try to constrain it, as well as amongst outsiders who wish to receive a clear, more or less unbiased, picture of the events.

Campaigning within social media and exercising power in it may seem very ambiguous. Anonymity which can almost be reached online gives great potential for exercising various types of power. However, there are a number of pitfalls to be avoided. One of these pitfalls is traceability or the lack of awareness about it. Many times it is difficult to trace a piece of information back to its source. A piece of information can become popular quickly, regardless of its truthfulness. Even if it is discredited at a later point, the damage to its subject's reputation has already been done. Even though we can assume that many people are aware that often the information on Internet is not very reliable.

Simultaneously one can be unaware of traceability. Information on Internet is traceable in a way that many users do not realize. Whether or not a piece of information is tracked to its source is simply a matter of effort and commitment. For example, a rumor which is traced back to its origin can boomerang and dishonor the originator.

In cyberspace information spreads much faster than it does through conventional media, be it truthful or not. Once posted online it may travel to different websites and platforms

on which it may become re-posted without any modifications or as slightly amended. This results in a vast amount of data about a single subject. The consequences are sometimes similar to the popular childhood "Phone Game": A whispered message is passed on in a line of people, and the longer the line is the more the message becomes modified. Often the message received by the last person in line has little to do with the original message. Even if the information is discredited afterwards, traces of it will persist in different forms accessible to anyone who can use a search engine.

A similar issue exists with regard to the vulnerability of systems such as e-mail servers. With enough technical know-how e-mail servers can be hacked and their revealing content may be published for everybody to see. On the other hand, it is also possible to forge e-mail conversations and present them as genuine.

Exercising hard power online can also be problematic. Partly this is so because Internet is sometimes thought to be a universally free zone and is compared to open seas in naval terminology. Restricting the access to Internet or to parts of it generally raises criticism. It can foster resentment and even riots within the parts of the population that were previously ambiguous towards political issues. Similarly, the use of technically rather uncomplicated tools, such as bots on Twitter, can result in aggravation amongst the less tech-savvy users simply because they might experience this method as a large-scale and technically advanced attack. This would have the "David facing Goliath"-effect which is not desired in a society that values democracy.

The article has identified a range of methods for political struggle and confrontation in social media. Depending on the cultural setting or the level of access to technologies, other aspects of the political struggle in cyberspace might prevail. However, in any case it is crucial for the government to carefully consider the methods with which it chooses to respond to an unrest rooted in social media, as well as the potential consequences of the methods used with regard to the overall political aims, desirable outcomes and the governmental capabilities.

The question of how the government deals with social media based events is a significant one. The nature of social media challenges the established, state-centric, viewpoint on exercising power. This article exemplified how power is exercised outside governmental control. As Internet becomes more accessible and the social networks residing within it grow, it becomes more important to research thoroughly its underlying mechanisms. In addition, it becomes ever more desirable for the governments to act within social media.

References

Arquilla, John; Ronfeldt, David. (2001) *Networks and Netwars: The future of terror, crime, and militancy*. Santa Monica, CA: RAND National Defense Research Institute.

BBC News. (2011a) *"Social networks to meet home secretary over riots".* BBC. Posted: 08/19–2011. Retrieved: 05/18-2012. (*http://www.bbc.com/news/technology-14587502*)

BBC News (2011b) "*Egypt: Hosni Mubarak fined for cutting Internet"*. BBC. Posted: 05/28–2011– Retrieved: 05/19–2012. (*http://www.bbc.co.uk/news/world-middle-east-13585237*)

BBC News. (2011c) *"Ряд российских сайтов подвергся атаке хакеров". ("A number of russian websites attacked by hackers").* Posted: 12/04-2011. Retrieved: 05/18-2012. Russian. (http://www.bbc.co.uk/russian/russia/2011/12/111204_echo_moskvy_ddos.shtml)

Dagens Nyheter. "*Nätilskan växer i Ryssland". ("Net angers grows in Russia")*. Dagens nyheter. Posted: 12/07–2011. Retrieved: 05/19–2012. Swedish. (*http://www.dn.se/nyheter/varlden/natilskan-vaxer-i-ryssland*)

Dodd, Vikram and Davies Caroline. "*London Riots Escalates as Police Battle for Control".* The Guardian. Posted: 08/09–2012. Retrieved: 05/19–2012. (*http://www.guardian.co.uk/uk/2011/aug/08/london-riots-escalate-police-battle*)

Forbes. *"Основателя «ВКонтакте» Павла Дурова вызвали в прокуратуру"*. (*"Founder of VKontakte was called into prosecutor's office"*) Forbes.ru. Posted: 12/09–2011. Retrieved: 05/19–2012. Russian. (*http://www.forbes.ru/news/77344-osnovatelya-vkontakte-durova-vyzvali-v-prokuraturu*)

Elder, Miriam. *"Polishing Putin: hacked emails suggest dirty tricks by Russian youth group".* Guardian. Posted: 02/07–2012. Retrieved: 05/18-2012 (*http://www.guardian.co.uk/world/2012/feb/07/putin-hacked-emails-russian-nashi*)

EHN. *"Russian Anonymous take down Kremlin and FSB sites".* E Hacking News. Posted: 10/05–2012. Retrieved: 05/18–2012. (*http://www.ehackingnews.com/2012/05/russian-anonymous-take-down-kremlin-and.html*)

Etling, Bruce. *"Massive DDOS attack on Independent Media during Russian Duma Election".* Harvard University Internet and Democracy Blog. Posted: 12/04–2011. Retrieved: 05/19–2012. (*https://blogs.law.harvard.edu/idblog/2011/12/04/massive-ddos-attack-on-independent-media-during-russian-duma-election/*)

Gasparov, Mihail, (Михаил ГАСПАРОВ) *"В Москве попробовали twitter-революцию" (Moskva tried twitter-revolution).* Утро (utro). Posted: 12/05-2011. Retrieved: 05/19–2012. (*http://www.utro.ru/articles/2011/12/05/1015089.shtml*)

Gazeta. *"Вслед за «Коммерсантом» в день митинга DDoS-атаке подверглись «Эхо», «Дождь» и Slon.ru". ("Kommersant, Ekho, Dozhd and Slon.ru were subjects to a DDoS attack on the day of the protest"*) Posted: 05/06–2012. Retrieved: 05/19–2012. Russian. (*http://www.gazeta.ru/politics/news/2012/05/06/n_2329873.shtml*)

Goncharov, Maxim. (2011) "*The Dark side of Social Media"*. Malware blog. Trend labs. Posted 12/07–2011. Retrieved 05/19–2012– (*http://blog.trendmicro.com/the-dark-side-of-social-media/*)

Guynn, Jessica *"British riots: Cameron considers ban on social networks"*. LA Times. Posted: 08/11–2011. Retrieved: 05/18–2012. (*http://latimesblogs.latimes.com/technology/2011/08/cameron-considers-blocking-facebook-twitter-after-riots.html*)

Halliday Josh (2011a) "*London Riots: BlackBerry to help Police probe Messenger Looting 'role*" The Guardian. Posted: 08/08–2011. Retrieved: 05/19–2012. (*http://www.guardian.co.uk/uk/2011/aug/08/london-riots-blackberry-messenger-looting*)

Halliday Josh (2011b) "*London Riots: How BlackBerry Messenger played a Key Role*" The Guardian. Posted: 08/08–2011. Retrived: 05/19–2012. (*http://www.guardian.co.uk/media/2011/aug/08/london-riots-facebook-twitter-blackberry*)

Harvard Kennedy School. (2008) *"Joseph Nye on Smart Power".* Posted: 06/03–2008. Retrieved: 05/18–2012. (*http://www.hks.harvard.edu/news-events/publications/insight/international/joseph-nye*)

Hounshell, Blake. (2011) "*The Revolution Will Be Tweeted*." Published online. Foreign Policy. Retrieved: 05/18–2012. (*http://www.foreignpolicy.com/articles/2011/06/20/the_revolution_will_be_tweeted*)

Infosecurity Magazine. "DDoS-vidaniya: Anonymous takes Kremlin off-line". Posted: 11/05–2012. Retrieved: 05/19–2012. (*http://www.infosecurity-magazine.com/view/25734/ddosvidaniya-anonymous-takes-kremlin-offline/*)

Keen, Andrew. "*How Russia's Internet 'hamsters' outfoxed Putin"*. CNN. Posted: 12/13–2011. Retrieved: 05/19–2012. (*http://edition.cnn.com/2011/12/13/opinion/andrew-keen-russia/index.htm*l)

Lindquist, Kristina. "*Det är rätt att göra uppror - fast helst på nätet"*. (*"It's right to rise up - preferably on-line"*). Dagens Nyheter. Posted: 10/16–2011. Retrieved: 05/18–2012. Swedish. *(http://www.dn.se/kultur-noje/det-ar-ratt-att-gora-uppror--fast-helst-pa-natet)*

Lonkila, Markku (2012), "*Russian protest on- and offline; the role of social media in the Moscow opposition demonstrations in December 2011*". Finnish Institute for Foreign Affairs.

Newsru.com. *"Хакеры активизировались в день выборов: под атакой "Эхо Москвы", "Голос", "Коммерсант", The New Times*". ("*Hackers active on election day: "Ekho Moskvy", "Golos", "Kommersant" and The New Times under attack*"). Posted: 12/04–2011. Retrieved: 05/19–2012. Russian. (http://www.newsru.com/russia/04dec2011/ddos.html)

Nummelin, Wiktor. "*Putin pressas efter val som kantas av beskyllingar om valfusk*" ("*Putin under pressure after an election surrounded by allegations of fraud*"). Dagens Nyheter. Posted: 12/05–2011. Retrived: 05/19–2012. Swedish. (*http://www.dn.se/nyheter/varlden/putin-pressas-efter-val-som-kantas-av-beskyllningar-om-fusk*)

Nye, Joseph S. (2004) *Soft power: the means to success in world politics.* New York, NY: Public Affairs.

Nye Jr, Joseph S, (2009) "*Get Smart; Combining Hard and Soft Power*", Published online. Foreign Affairs July/August 2009. Retrieved 05/18–2012. (*http://www.foreignaffairs.com/articles/65163/joseph-s-nye-jr/get-smart*)

Obama, Barack (2011) "*Remarks by the President on Situation in Egypt*". The White House. Posted: 01/28–2011. Retrieved: 05/19–2012. (*http://www.whitehouse.gov/the-press-office/2011/01/28/remarks-president-situation-egypt*)

Oxford dictionaries. (2012) *"Slactivism" Oxford University Press.* Retrieved 05/18–2012. (*http://oxforddictionaries.com/definition/slacktivism*)

Portalinski, Emil. "*Russians use Facebook to protest alleged election fraud". ZDNet. Posted: 12/08–2011. Retrieved: 05/19–2012. (http://www.zdnet.com/blog/facebook/russians-use-facebook-to-protest-alleged-election-fraud/5975)*

Rotman, Dana. ed. (2011) "*From slacktivism to activism: participatory culture in the age of social media".* Proceedings of the 2011 annual conference extended abstracts on Human factors in computing systems. New York: ACM. P. 819–822. Retrieved: 05/18–2012. (*http://dl.acm.org/citation.cfm?id=1979543*))

Rusecurity. *"Боты Твиттера глушат анти-кремлевские твиты".* (*"Twitter bots drown out anti-kremlin tweets"*). Rusecurity. Posted: 12/08-2012. Retrieved: 05/19–2012. Russian. *(http://www.rusecurity.com/2011/12/08/botyi-tvittera-glushat-anti-kremlevskie-tvityi/)*

SecurityLab. *"Масштабные DDoS атаки на сайты российских СМИ".* (*"Large-scale DDoS attacks against websites of Russian mass-media"*"). Posted: 05/06–2012. Retrieved: 05/19–2012. Russian. (*http://www.securitylab.ru/news/424181.php*)

Soldatov, Andrei. *"Vladimir Putin's Cyber Warriors".* Posted: 12/9–2011. Retrieved: 05/19–2012. (*http://www.foreignaffairs.com/articles/136727/andrei-soldatov/vladimir-putins-cyber-warriors*)

Taylor, Adam (2012a) *"Is Vladimir Putin Behind An Army Of Internet Trolls?"* Business Insider. Posted: 02/07–2012. Retrieved: 05/18–2012 (http://articles.businessinsider.com/2012–02–07/europe/31032932_1_kremlin-nashi-mails)

Taylor, Adam (2012b) *"Ustream is Facing its Biggest DDOS attack Ever, Reportedly Targeting One Russian Opposition Account"* Business Insider. Posted: 05/09–2012. Retrieved: 05/18–2012__(*http://articles.businessinsider.com/2012-05-09/news/31636228_1_russian-protests-russian-president-vladimir-putin-denial-of-service-attack*)

Zhang, Yuzhi & Jiang, Zhongfu. (2010) "*The Domestic Governance Countermeasure in Order to Enhance Soft Power of China Communist Party*" Published online. International Journal of Business and Management. Vol. 5, No. 7; July 2010. Retrieved 05/18–2012. (*www.ccsenet.org/ijbm*)

Zuckerman, Ethan. (2011) *The First Twitter Revolution?* Published online. Foreign Policy. Retrieved: 05/18–2012. (*http://www.foreignpolicy.com/articles/2011/01/14/the_first_twitter_revolution*)

Victory in Exceptional War: The Estonian Main Narrative of the Cyber Attacks in 2007

Kari Alenius

Abstract

"Victory in Exceptional War" focuses on the large-scale cyber attacks Estonia fell victim to. For some the cyber attacks mark a milestone in modern warfare. The study does not declare whose perspective on the attacks is "right" and whose is "wrong". Instead, it will analyse published Estonian interpretations of what occurred and argues that the most essential element in the popularisation of the attacks was that the events were seen as a war with all its classical characteristics. In this context, actions of one's home nation were perceived as a successful repulse to enemy attacks and a foreign country (Russia) was perceived as an attacker. At the same time, the universal features of an enemy were utilised in the construction of the opposing party.

Keywords: rhetoric, narratives, cyber attack, Estonia

Estonian Public Discussion as a Starting Point for Analysis

The Internet resources of Estonia's leading media outlets *Eesti Päevaleht* (EPL), *Postimees* (PM), *Õhtuleht* (OL), *Eesti Rahvusringhääling* (ERR) were examined from the end of April 2007 to the end of June 2007 for this study. In addition, a Google search for on-line material was conducted by using the keywords *cyber-attack, Estonia, 2007* – and their Estonian equivalents. In this way, individual published speeches were found from among other publications and from the home pages, for instance, of the Estonian state institutions. In the case of the four aforementioned media outlets, it is evident that the Google search yielded almost exactly the same results as the systematic review of the Internet newspaper archives. Thus, it can be concluded that the most salient Estonian Internet data has been analyzed in this study. On the other hand, this study only analyzes the Estonian media discussion which necessarily cannot be equated with the perceptions held by the wider public in Estonia.

The aim of the study is to find out what kinds of narratives were created about the events in Estonia and to explain why these narratives were of a particular kind. In a nutshell, it can be said that with a "narrative" scholars usually refer to texts and oral presentations that have a storied form. The creators of narratives interpret the world and construct tales with diverse degrees of organization and logic. Individuals, various interest groups and nations select, connect, evaluate and explain events, and turn them into meaningful stories that are intended to meet the needs of a particular audience, which often includes the creators themselves (Riessman, 2005, 1; for a more detailed analysis of narrative approaches and their possible applications, see for instance Rantapelkonen, 2006, 48–77).

As an alternative to narrative we might speak of certain types of discourses or mental images. Regardless of the selected term the question is about the examination of the processes that essentially guide human activity. Multiple sciences have convincingly demonstrated that above all people act on the basis of their mental impressions and not on the basis of "objective facts" that are empirically observable – although the former are of course built upon the latter. In many ways, mental images, as well as narratives, are stereotypical, in other words, simplified and coloured models of reality. For the most part, they arise as a result of largely unconscious and, to a more minor degree, of conscious psychological processes (Fält, 2002, 8–10; Ratz, 2007, 189–195).

Along with empirical findings, mental images are influenced by an individual's beliefs, fears, hopes, and all of the factors behind the aforementioned – in short, the whole experiential history of an individual and his or her perception of the world. If a group of people shares certain images of a subject we can speak of collective images. Narratives and discourses partly reflect the mental impressions that already exist. They are also partly used for constructing images, clarifying images for oneself, and spreading them to other people (Fält, 2002, 9–11; Ratz, 2007, 199–213). In any case, the importance of mental images in interaction between people and throughout the course of history justifies why, in the case of Estonia's cyber attacks of 2007, it makes sense to analyze mental images and narratives created by the events. Even if these narratives are not necessarily "true" people tend to regard them as true. As a consequence, they become real at the level of consequences and further influences.

Cyber Attacks in 2007 and Their Contexts

To understand the narratives generated, it is reasonable, first, to briefly explain the actual events and their associated contexts. The cyber attacks were related to Estonia's so-called Bronze Soldier uproar. In 1947 the Soviet Union had set up a military statue in the center of Estonia's capital, Tallinn. The official name of the statue was "a monument to the liberators of Tallinn". After the Estonian independence (1991), the fate of all Soviet monuments came into question. The Bronze Soldier was left in place, but it became a memorial for all those who had fallen during the WWII. However, these changes did not prevent the statue from becoming the focus of disputes. Some Estonian Russians organized annual celebrations near the statue on the 9th of May, Russia's so-called Victory Day, as well as on the 22nd of September, the anniversary of Tallinn's "liberation". In the minds of many Estonians, these kinds of celebrations were hostile actions towards Estonia because on the Estonian side the statue was often regarded as a symbol of the Soviet occupation. From the Estonian perspective, the open show of Russian and Soviet symbols during the celebrations was a glorification of the occupation and a distortion of history. In September 1944, the occupier only changed and there was no "liberation". (Kaasik, 2006, 1893-1916).

On the 9th of May 2006, there was a confrontation by the statue in which Russian celebrators attacked protesters carrying the Estonian flag. After the conflict, demands that the statue should be removed from Tallinn's center and placed elsewhere strengthened. In the beginning of 2007, the Estonian parliament adopted two laws on the basis of which the Bronze Soldier and other similar monuments, as well as any dead buried in connection with them, could be moved to a more suitable location. Preparations to move the Bronze Soldier and the Soviet

soldiers buried nearby began on the 26th of April 2007. The statue and its surroundings were isolated with fences and unauthorized access to the site was blocked. In the same evening, Russians opposing the operation were involved in large-scale rioting and sabotage in the center of Tallinn, and the unrest continued in the following night. The Bronze Soldier was moved as planned to Tallinn's military cemetery and opened to the public on the 30th of April, and the situation in Tallinn calmed down (RKK, 2007, 1–3).

At the same time as the riots took place, targeted cyber attacks against Estonia began on the 27th of April. These attacks targeted mainly the websites of the Estonian state institutions. The attacks consisted mainly of massive spamming and DDOS attacks. On the last day of April, the extent and technical level of the attacks rose sharply and the DNS system of the Estonian servers became the main target. The number of the attacked sites increased and expanded to include Estonian Internet service providers and the Estonian media. The attacks continued in varying intensity on a daily basis until mid-May (May the 16th), after which the situation returned to almost normal. Most of the cyber attacks came from Russia, and the technical factors of and the large-scale resource requirements for these attacks suggest that the Russian government was involved. The Russian state naturally denied any involvement (RKK, 2007, 2–4; Saarlane, 2007–05–17).

Russia has also denied responsibility for other aggressive actions against Estonia. However, as early as the beginning of 2007, Russia's state leadership warned Estonia about moving the Bronze Soldier, and on the 23rd of April, it left a formal diplomatic note about the issue to Estonia (ERR, 2007–04–27). Already before the relocation of the statue there had been intensifying anti-Estonian verbal attacks in the state-controlled Russian media, and during the riots the Russian Embassy in Tallinn, at the very least, kept close ties with the leaders of the riots. In Moscow, anti-Estonian protesters surrounded the Estonian Embassy for a week, apparently with the consent of the government, and prevented it from operating normally. In practice, Russia also undertook economic sanctions against Estonia and began a boycott of Estonian products in Russia, although the Russian government also sought to explain these actions as the result of unrelated factors and circumstances (RKK, 2007, 3–4).

State Leadership, Journalists and IT Professionals Representing the Main Narrative

When the reaction of the Estonian public to these cyber attacks is examined, it is evident that quite soon after the onset of the attacks the public debate began to develop two rival narratives. On the one hand, there was the mainstream public debate which can be called *the main narrative* and, on the other hand, there was a competing narrative that received less publicity and which can be called *the counter narrative*. The main narrative was represented by Estonia's state leadership, as well as by the majority of journalists and IT professionals who publicly commented on the issue. The creators of the counter narrative consisted of a few individual commentators who belonged to the latter two groups.

During the first three days of the cyber attacks uncertainty and confusion prevailed among the Estonian public, which did not provide sufficient conditions for the birth of a narrative. In the first few days, the main focus was on the riot and on its aftermath, which

is understandable as this had never before happened in Estonia. Moreover, because of its drama the event had a high news value. In the next couple of days, relatively few cyber attacks occurred and no clear information was available on their nature and origin. The issue was also new and unexpected: the attacks had not been anticipated, and there were no precedents in Estonia or elsewhere in the world on the basis of which an image could have been built immediately. Thus, public uncertainty and confusion was apparent in that the news media took a neutral tone regarding the matter. For example, the news media reported that the websites of the Estonian state institutions had been attacked or were being harassed, but other evaluations of these events were not presented (ERR, 2007–04–28; ERR 2007–04–29).

The birth of the main narrative can be considered to have taken place on the 30th of April; the date on which the first indicative commentaries appeared (OL, 2007–04–30; Virumaa Nädalaleht, 2007–04–30). Over the following two weeks, the mainstream image and the narrative of the incident broadened and took its essential form. During the second half of May, a few additional elements related to the end of the attacks were added to the main narrative. Then, there were more time and better conditions for drawing conclusions and forming an overall picture. However, the most active phase in the public debate took place in mid-May, and from the perspective of the media, the actuality of the topic began to wane after this. During the summer and fall of 2007, the topic was rarely returned to in the Estonian public. Nonetheless, the main narrative only took its final form during this time period.

The declaration of Estonia's Justice Minister Rein Lang to the Estonian television on the evening of the 30th of April acted as the initiator of the main narrative. Lang stated that investigations into the IP addresses of the attackers had revealed that the attacks originated in Russia and that, among others, some government institutions in Moscow were involved (OL, 2007–04–30). During the following couple of days, one of the basic elements crystallized in the Estonian public discussion: Russia was the attacker (Delfi, 2007–05–01; OL, 2007–05–03). Albeit a few news reports stated that majority of the attacks came from other addresses than those under the direct control of the Russian government, and even if the so-called botnet technique hampered the clarification of the origin of the attacks, the guilty party was now known (ERR, 2007–05–04).

If the Russian state did not itself organize the attacks, it was responsible for them as, according to the interpretation of the Estonian media writers, it could have chosen to prevent them. Additionally, "Russia" was guilty because in any case the attacks came from there – were they then implemented privately or by the government (Delfi, 2007–05–01; OL, 2007–08–09). The conclusion that Russia was guilty was probably affirmed by other circumstantial evidence, such as the earlier threats and verbal attacks against Estonia by the Russian government leaders and the media, as well as Russia's suspected involvement in the rioting – at the very least as an instigator and, where necessary, as an advisor.

The identification of an enemy was a relief to Estonians, as afterwards it was easier to interpret the situation and more possible to design countermeasures – at least, at the level of beliefs. A vague and faceless enemy is always experienced as more fearsome (Zur 1991, 345–347). In question was a general human psychological reaction, which a commentator

descriptively put into words at the beginning of May: "...The issue also has a good side. Events on the streets of Tallinn illustrate who our enemies are, and how many of them there are. There are no more illusions. Enemies cannot be integrated" (Delfi, 2007–05–01).

When an enemy for the main narrative had been found, the construction of the narrative could begin. Almost inevitably the building was done by using the logic and structure of the general image of the enemy. Since this was a new type of situation which did not fully recall the traditional war (for instance, an official declaration of war and the conventional use of military force were lacking), all of the typical elements in the image of the enemy could not be used. Nevertheless, a few main elements were included in the Estonian main narrative. Firstly, the terminology used portrayed a war and an enemy. There was an enemy that attacked and one's own country which repelled these attacks. A clear polarization between "us" and "others" is necessary in perceiving the existence of an enemy or another party (Zur, 1991, 345–346).

Secondly, the perception of the enemy is related to clear valuations of "good" and "bad". One's own side represents the good and acts properly, while the other party represents the bad and acts incorrectly, both on a theoretical–moral and on a practical level (Zur, 1991, 345–353). Following this polarization of values there was no understanding shown in the Estonian public for the acts of the enemy but those were categorically condemned. Usually, there is no room for pondering the actions of the enemy in the sense that consideration would be given to why the enemy views the conflictual situation in a different way, and could the enemy, from his or her point of view, have any "reasonable" or even "legitimate" grounds for his or her actions. In the mainstream Estonian public debate those responsible for these cyber attacks were explicitly wrong, malicious, and criminal (Delfi, 2007–05–01; ERR, 2007–05–05; Arvutikaitse, 2007–05–09).

Thirdly, a particular characteristic adopted in the Estonian main narrative can be considered the typical manner in which the strengths and weaknesses of the enemy are brought into light. An appropriate balance between strengths and weaknesses is always sought in portraying the enemy. The enemy must be sufficiently strong so that the threat to one's own side is taken seriously and that there is sufficient readiness to fight against the enemy, as well as if necessary, to make sacrifices in order to achieve victory. Simultaneously, victory over a strong enemy emphasizes the heroism and ability of one's own side and thus, acts as a mental factor in strengthening the community. However, in emphasizing the strength of the enemy one should not go too far, as if the enemy is portrayed too strong, it can result in hopelessness and defeatism within one's own community (Zur, 1991, 346–360).

In the mainstream Estonian debate, the strength of the enemy was emphasized by explaining openly and in detail how wide-ranging and how many types of cyber attacks had been conducted against Estonia. However, at the same time it was remembered to note that these attacks had been repelled. If in some cases the enemy had gained an advantage, this advantage was only temporary and limited. The counter-measures of one's own side had already gained control of the situation and no vital area had truly been in danger (ERR, 2007–05–01; OL, 2007–05–03). Thus, both the listeners and perhaps also the narrators of this narrative were able to feel safe in relation to the overall developments and the final result of the war.

One could also feel safe in regard to the fact that in spite of its strength the enemy was weak and inferior according to classic models of portraying an enemy. The aforementioned characteristics can occur, for example, in the ridiculousness of the enemy. A comparison that exploits the assumed negative characteristics of the enemy strengthens the opposing characteristics of one's own side. In the Estonian mainstream public debate, this element was reflected in the good-natured comments of a few IT professionals regarding the simplicity of some cyber attacks and the fact that they were easily deflected. The inability of the attackers to understand that their IP addresses were easily found and that they revealed themselves was also wondered publicly. No setbacks in these contexts were mentioned (ERR, 2007–05–04).

The Counter Narrative

In the competing narrative, the aforementioned issues were mostly denied or put in perspective. The common basic premise was that Estonia had ended up in difficulties. The critique was not so great that it would have questioned the belonging to the same community (Estonia/Estonians) or that the existence of the conflict would have been disputed. However, the description of details and their interpretations differed.

This counter model of interpretation did not interpret the Russian state as the main opponent. Nevertheless, this did not mean that the counter narrative would have taken a positive stance towards Russia; it just emphasized the difficulty of tracing the nature of the attacks as well as the role of individual Russian entities. In practice, the data available to the opposition was the same which the supporters of the main narrative utilised, but the supporters of the counter narrative thought that it justified lesser conclusions: the Russian state was not the mere responsible one. The intermittent success of the cyber attacks and one's own temporary insufficiency to respond to them were also highlighted (EPL, 2005–05–17; Elamugrupp, 2007–06–30).

In the minds of those supporting the counter narrative, the question was perhaps also that of war, but according to their interpretation, the issue was not only about a simple series of successful defences – like the matter was presented in the mainstream debate. In the most extreme, the Estonian defenders against the cyber attacks were accused of overreacting and even unknowingly playing into the hands of the enemy: if the goal of the enemy was to isolate Estonia from the rest of the world, then the Estonians had ultimately done this by themselves by blocking the access of foreign Internet addresses to Estonian websites. This assumedly successful countermeasure, the "efficient" prevention of spam and DDOS traffic, had led into a situation in which the enemy achieved what it had wanted. (EPL, 2007–05–17).

There were relatively few statements that built on the counter narrative in the Estonian public debate, that is, about one tenth of all news and commentary relied on it. There was roughly the same number of statements belonging to a "gray zone", and it is difficult to classify these statements into either of the groups. Therefore, about eighty percent of all of the statements belonged to the group that built on the main narrative. There were no differences between the publications in regard to what kinds of statements were published; for example, there

were no significant differences between Estonia's leading Internet publications. Individual supporters of the counter narrative could be found within different publications instead of having concentrated in any of them.

The journalists who supported the counter narrative were possibly practicing a culture that is characteristic to conditions in which free exchange of information prevails; particularly, to the conditions in Western democracies. A few researchers have referred to this phenomenon as symbolic shadow-boxing. In conditions where there is a freedom of information, it is considered the duty of the media to provide the general public with an image that is not too uniform – regardless of the issue and the situation. If differences of opinion and differing interpretations of the "facts" are not born otherwise, self-respecting journalists must create them – if necessary, in the name of criticality and pluralism. This can lead directly to the aforementioned shadow-boxing, although the basic configuration of the crisis and the justification for defending one's own side are usually not put into question. However, it is considered necessary to search for mistakes and failures in one's own actions. (Carruthers, 2000, 157–158.)

Additional Characteristics and Further Development in the Main Narrative

The key characteristics of both of the aforementioned narratives were created and established by mid-May. After this, there was no apparent formation of additional characteristics in the counter narrative, which is partly due to the fact that later on there were very few statements belonging to this narrative. Because these late comments were so few, it impossible to make any broader conclusions regarding the possible changes in position (Vikerkaar 2008). In the case of the main narrative, however, it is possible to continue with an analysis of the further developments. By the second half of May, two additional characteristics had joined the image. During the summer and fall of 2007, the image crystallized to take the shape of a few general interpretations.

The first additional characteristic was that by the end of May, it was already ventured to declare that Estonia was the victor of the war. No significant cyber attacks had occurred for a week, and from the perspective of the daily attacks that had occurred by the end of April and at beginning of May, this seemed as sufficient evidence to end the war. On the other hand, as the logic of the enemy images entails, one's own side has no reason to lull itself with a false sense of security. Once the enemy has been found he or she continues to be a potential enemy, and it is unrealistic to wish for a world without an enemy. It was remembered to emphasize in the main narrative that the attacks against Estonia and elsewhere were possible, even probable, in the future. For this reason, the Estonians had to remain vigilant and develop their capacity to combat future attacks (OL, 2007–05–17; EPL, 2007–05–25).

The second additional characteristic was closely related to the first one. In principle, it contained two conflicting sides of the same issue. On the one hand, it was reported that Estonia was an object of admiration for NATO allies, and the statements of the Allied representatives visiting Estonia were quoted frequently in public. Accordingly, the guests

came to learn from the Estonians (Äripäev, 2007–05–18; PM, 2007–05–25). Praise received from others is always pleasant and it helps to construct a positive image of oneself or of one's own group; to this extent, the quotation of statements had a clear general psychological background. On the other hand, several Estonian statements which otherwise clearly belonged to the main narrative emphasized the need to gain support in rebuffing the cyber attacks. Speeding up the construction of NATO's cyber defense center in Estonia (which had already been agreed on in 2004) was met with joy and, additionally, there was a desire for an international reform regarding the definition of cyber attacks. It was considered that the existing international agreements were outdated for they did not take the matter seriously enough, did not take into account the technological development in the field, nor did they allow for a sufficiently effective legal and practical response on the basis of international cooperation (PM, 2007–05–14; Virumaa, 2007–05–25).

It is clear that the achievement of international agreements and definitions that would obligate other countries to assist states that have become the target of cyber attacks would have been to Estonia's advantage. For this reason, it was reasonable for the representatives of Estonia to demand this in both Estonia's internal debate as well as abroad (EP, 2007–05–10). At the same time, assistance, in particular from other NATO countries, would have been welcome. In principle, however, it was questionable what assistance would have been available from other countries if Estonia was already the world's leading expert in cyber defence, which, for example, the representatives of the U.S. military came to admire in the role of apprentice. This paradox was not mentioned in the Estonian statements. According to the principles of propagandistic communication, contradictory elements can be used in communication – as long as they are not presented at the same time (Zur, 1991, 350–351). Thus, in the Estonian main narrative these two things – Estonia in need of assistance and Estonia as the world's most skilled nation in cyber defence – never appeared in the same statements.

On the international scene, defining the cyber attacks as a war was driven, especially, by the Estonian president Toomas Hendrik Ilves and the Estonian members of the European Parliament (EP, 2007–05–10; President, 2007–06–18). For them, based on their positions and contacts, driving the national interests of Estonia abroad naturally fit well. Simultaneously, their positions were also heard by the Estonian public. The same message was forwarded particularly to the domestic audience by the speaker of the Estonian parliament Ene Ergma (EPL, 2007–05–25). When the commander of the Estonian armed forces Ants Laaneots is added to the list of leading constructors of the main narrative, it can be said that Estonia's highest state leadership was more or less in favor of the main narrative. Out of all Estonia's influential public personas Laaneots (PM, 2007–06–20), as well as the former Prime Minister and the later Chairman of the leading right-wing party (IRL) Mart Laar (OL, 2007–08–09) most clearly stated that the Russian state was responsible for the cyber attacks. Ilves and Ergma expressed the matter more diplomatically, but even in their statements there was no doubt about the main opponent in the war.

Conclusion

As said earlier, the central elements of the main narrative crystallized during the summer and fall of 2007, so that over time the details and the exact course of the events became side issues. Detailed and exact components fell or were dropped from the narrative and the image which increasingly became composed of a few key elements describing the entire conflict in general terms and in a stereotypical way. For instance, one's own side and the opposing side were both seen through a clear black and white dichotomy, and the opponent featured the universal characteristics of an enemy. All in all, it can be concluded that according to the Estonian main narrative the cyber conflict consisted of the following components: 1) it was a war; 2) the Russian state was either directly or indirectly responsible for the attacks; and consequently, Russia was seen as the enemy in the war; 3) in question was a new, unprecedented kind of war; and 4) the war ended in victory for Estonia.

Approximately eighty percent of the Estonian public debate either built on or supported the main narrative. In this sense, it can be regarded as a strong national narrative. The fact that in its content it had a strong nationalistic emphasis and that its most visible supporters were individuals who belonged to a conservative right-wing also makes it a national narrative. As in many cases the same individuals belonged to Estonia's state and political elite, the main narrative can, to a large extent, also be described as Estonia's official narrative. However, it was not a case of the Estonian government forcing members of the elite or the Estonian media to comply with this explanation. It was sufficient that the situation and the conditions were such that the majority of those who participated in the public debate came to similar conclusions on their own initiative. The experience of the Estonian society coming under an unfair attack from the outside gave birth to a very large and uniform defensive reaction which was first explained to oneself (the Estonians) and then to others (world opinion) with the help of the main narrative.

The counter narrative was perhaps formed as a conscious counter-reaction to the main narrative. The main narrative may have been experienced as too uniform and hence propagandistic or implausible. It may also have been a case of differences in interpretation regarding other events and hence without any initial purpose of criticizing the mainstream narrative. The counter narrative questioned the nature of the events as a war and preferred to support the interpretation of the events as Internet harassment. Simultaneously, the interpretation which regarded the Russian state as the opponent in the crisis was viewed as too simplistic and the private or unclear background of the attackers was emphasised. The exceptionality of the events was also questioned and they were compared to known, large-scale operations of harassment and damage initiated by private parties; particularly, in the field of economic competition. Similarly, the fourth main characteristic of the main narrative, victory in the war, was not seen as a legitimate interpretation: if there was no war there was also no victory. In addition, the success in combating the operations varied according to this view.

In principle, both of the narratives were based on the same information on the events. Both of them were also partly built on the basis of general psychological models, in which the role of the apparent "facts" in shaping the narrative lessened. The narratives used empirical construction materials, but their development partly followed models guided by

a stereotypical, human way of thinking. Thus, for instance, the images of the enemy are generally similar regardless of the circumstances. The appropriate selection and interpretation of the available information was essential so that it supported the perceived best, simple enough explanation of the model – a narrative. It is impossible to determine the relative weight of both conscious and unconscious activity, but they both have undoubtedly played a significant part in the birth of these models. To uncover the specific characteristics of these narratives, the content of the media coverage in the neighboring countries (for instance, the Baltic and the Scandinavian countries) during the same time period should be examined. Yet this requires a separate study in the future.

References

Äripäev (2007-05-18) 'Eestist saab NATO kübersüda ja IT-polügoon', http://leht.aripaev.ee/?PublicationId=464dc490-fb94-4024-9b75-258ddc8543a9&articleid=12282&paperid=A4DE138A-6A0D-4C2A-A1B6-6613E673D67A

Arvutikaitse (2007–05–09), '9. maid tähistati küberrünnakuga', http://www.arvutikaitse.ee/9-maid-tahistati-kuberrunnakuga/

Carruthers, S. (2000) *The Media at War: Communication and Conflict in the Twentieth Century*, Basingstoke: Macmillan

Delfi (2007–05–01) 'Küberrünnak Eesti riigiasutustele', http://www.delfi.ee/archive/kuberrunnak-eesti-riigiasutustele.d?id=15733528

Elamugrupp (2007-06-30), 'Vaenlane kasutas kübersõjas müstilisi e-pomme', http://www.elamugrupp.ee/modules.php?op=modload&name=News&file=article&sid=1067&mode=thread&order=0&thold=0

EP (2007-05-10), 'EP palub Euroopa Liidul näidata üles solidaarsust Eestiga', http://www.europarl.europa.eu/sides/getDoc.do?type=IM-PRESS&reference=20070507IPR06398&language=ET

EPL (2007–05–17) 'Sõja versioon 2.0 (beeta)', http://www.epl.ee/news/arvamus/article.php?id=51087289

EPL (2007–05–25) 'Ergma: Eesti vastu suunatud küberrünnak ei jää EL-is viimaseks', http://www.epl.ee/news/eesti/ergma-eesti-vastu-suunatud-kuberrunnak-ei-jaa-el-is-viimaseks.d?id=51088437

ERR (2007–04–27) 'Venemaa andis Eesti suursaadikule pronksmehega seoses noodi', http://uudised.err.ee/index.php?0573764

ERR (2007–04–28) 'Valitsuse kommunikatsioonibüroo hoiatas valeteabe eest', http://uudised.err.ee/index.php?0573960

ERR (2007–04–29) 'Välismaised rünnakud häirivad valitsusasutuste veebilehti', http://uudised.err.ee/index.php?0574001

ERR (2007–05–01) 'Rünnakud Eesti küberruumi vastu on sagenenud', http://uudised.err.ee/index.php?0574069

ERR (2007–05–04) 'IT-ekspert: Vene rünnakud serveritele on oskamatult tehtud', http://uudised.err.ee/index.php?0574202

ERR (2007–05–05) 'Politsei pidas kinni esimese küberrünnakus osaleja', http://uudised.err.ee/index.php?0574259

Fält, O. (2002) 'Introduction', in Alenius K., Fält O. and Jalagin S. (eds.) *Looking at the Other. Historical Study of images in theory and practice*, Oulu: Oulu University Press.

Kaasik, P. (2006) 'Tallinnas Tõnismäel asuv punaarmeelaste ühishaud ja mälestusmärk', *Akadeemia*, no. 4.

OL (2007–04–30) 'Rein Lang: küberründed Venemaalt tulevad riiklikelt aadressidelt', http://www.ohtuleht.ee/227560

OL (2007–05–03) 'Venemaa küberrünnak Eesti pihta on Euroopa kohta tavatu', http://www.ohtuleht.ee/227851

OL (2007–05–17) 'Kübersõda karmistub', http://www.ohtuleht.ee/230007

OL (2007–08–09), 'Uurimise takistamine tõestab, et küberrünnak lähtus Venemaalt', http://www.ohtuleht.ee/241417

PM (2007–05–14) 'Aaviksoo rääkis NATO juhiga küberrünnakutest', http://blog.postimees.ee/170507/esileht/siseuudised/260640.php

PM (2007–05–25) 'USA eksperdid: küberrünnak Eesti vastu äratas meid', http://rooma.postimees.ee/040607/esileht/siseuudised/262679.php

PM (2007–06–20) 'Venemaa muutub Eestile üha ohtlikumaks', http://rooma.postimees.ee/210607/esileht/siseuudised/267665.php

President (2007–06–18), 'Toomas Hendrik Ilves: "Kas küberrünnak on hädaolukord?', http://www.president.ee/et/meediakajastus/intervjuud/3150-vabariigi-president-ajalehele-frankfurter-allgemeine-zeitung-18-juunil-2007/index.html

Rantapelkonen, J. (2006) *The Narrative Leadership of War. Presidential Phrases in the 'War on Terror' and Their Relation to Information Technology*. National Defence University. Department of Leadership and Management Studies. Publication Series 1. Research n:o 34, Helsinki, National Defence University

Ratz, D. (2007) 'The Study of Historical Images', *Faravid*, vol. 31.

Riessman, C. (2005) 'Narrative Analysis', in Kelly N., Horrocks C., Milnes K., Roberts B., and Robinson D. (eds.) *Narrative, Memory and Everyday Life*, Huddersfield, University of Huddersfield

RKK (2007) 'Moskva käsi Tallinna rahutustes', Rahvusvaheline Kaitseuuringute Keskus, http://www.icds.ee/index.php?id=73&tx_ttnews%5Btt_news%5D=179&tx_ttnews%5BbackPid%5D=99&cHash=a1145105e4

Saarlane (2007–05–17), 'Kreml eitas osalust Eesti küberrünnakutes', http://www.saarlane.ee/uudised/uudis.asp?newsid=29727&kat=3

Vikerkaar (2008), 'Küberrünnakute moos aprillirahutuste kibedal pudrul', http://www.vikerkaar.ee/?page=Arhiiv&a_act=article&a_number=4732

Virumaa (2007–05–25), 'VE: küberrünnakud', http://www.virumaa.ee/2007/05/ve-kuberrunnakud/

Virumaa nädalaleht (2007-04-30), 'Minister Rein Lang: küberründed tulevad Venemaa riiklikelt IP-aadressidelt', http://www.vnl.ee/artikkel.php?id=6804

Zur, O. (1991), 'The love of hating: the psychology of enmity', *History of European Ideas*, vol. 13, no. 4.

PART II:

Cyber Security

The Origins and the Future of Cyber Security in the Finnish Defence Forces

Anssi Kärkkäinen

Abstract

This article reviews the development of both cyber security and cyber defence within the Finnish Government and the Defence Forces over the past decades. It depicts the development from information and network security to modern cyber defence. Cyber security and defence issues have become more and more interesting in the global context over the past years. Many nations perceive cyber defence as a very critical area of development in the near future and thus, allocate resources to it. Like other nations, Finland has begun to prepare a national cyber security strategy. The strategy will also guide the Defence Forces. This paper reviews the current situation of the cyber defence development, and presents some future trends of cyber security that are likely to take place in the Finnish Defence Forces.

Keywords: Cyber security, cyber defence, defence forces, information security

Introduction

We read about cyber security events almost every day. These small pieces of news show how dependent we are on information technology, services and networks. Every actor, business, governments, military, and even individuals are more dependent on Internet than ever before. The critical infrastructure, including energy, banking and finance, transportation, communication, and health care system, rely on cyberspace consisting of both software and hardware that are still vulnerable to disruption or exploitation. Internet is open to everyone, and there are several motivations to use network access for aggressive, hostile purposes. The cost of using or developing cyber tools is incredibly low. In addition, the potential benefits gained from attacking are worth of trying and outweigh the dangers. This has led to what many call cyberwar.

Cyberwar is one of the growing threats to the modern armed forces around the world. There is no unanimous definition to cyberwarfare, but in the WSTIAC Quarterly Report (2009)[1] cyberwarfare is defined as any act intended to compel an adversary to fulfil a national will, executed against the software controlling processes within an adversary's system. Cyberwarfare comprises the following modes of cyber attack: cyber infiltration, cyber manipulation, cyber assault, and cyber raid. Cyber defence is the military aspect to cyber security. Some sources define cyber defence as defensive functions and the protection of information system, but in Finland the term cyber defence[2] is referred to in a way that includes all military actions taken to protect, attack, or exploit our own or an adversary's information and computer systems. Cyber defence is one of the operational capabilities. The aforementioned definitions are still

1 "Cyber Warfare - Understanding the Threat to Weapon Systems…", 2009.
2 Muuriankkuri, kesä 2012.

unofficial, but it is believed that the national cyber security strategy, which at the time of writing was still forthcoming, will clarify them.

Cyberwarfare is challenging, but it also brings forth new opportunities. The great powers began to develop these capabilities already years ago, and the smaller countries have later noticed the opportunities inherent in the cyber domain. Thus, it is very natural that also Finland is developing cyber defence capabilities. This article reviews the past development of information security, and its transformation into cyber security and defence. The purpose of the article is to show how Finland and the Finnish Defence Forces have developed the management and organizations of information security over the past decades, and what are the foreseeable trends in the near future.

The paper is divided into six sections. The first section is introduction, and the second briefly explains the evolution of cyberwarfare. The third section focuses on the development from information security to cyber security. The fourth section states the current situation of the governmental cyber security and cyber defence, and in the fifth section, the future trends are discussed. The sixth section concludes the paper.

Background – The Evolution of Cyberwarfare

Revolutions in science and technology have been major steps in human history. For example, the steam engine was a revolutionary invention replacing human muscles in several industrial areas. Steam engines enabled mass production and lowered the prices of daily groceries. Today, we are in the middle of information revolution. The computational power of modern computers facilitates things that we could not even imagine a few decades ago. The computers process calculations faster than the human brain can do. The computers and networks have formed a new virtual dimension on which a large proportion of our daily lives is dependent. Along with the development of Internet and other information networks and services, threats on these systems have increased. The scope is no longer to protect only information, but the whole virtual cyber environment of which functioning is vital to us. Thus, cyber security is transformed from a technical discipline to a strategic concept.[3]

After the institutional computer systems, the arrival of personal computer (PC) made a huge change to the way in which computers were going to be used. In the early 1940s, IBM's president Thomas J. Watson reputedly said that there was a world market for about five computers[4]. This legendary misjudgement shows how prediction has always been difficult, and how the inventors of the computer were unable to see it as a personal device. However, the number of computers began to increase and their efficiency was multiplied in a short period of time. Already in 1965, G. Moore correctly predicted that the number of transistors on a computer chip would double every two years[5]. Currently, the physical limits of the computer chips are approaching, as electronic circuits are reaching their minimum physical size.

3 Geers, 2011.
4 Bellaver, 2006.
5 Moore's Law, www.intel.com.

Albeit the physical limits are getting close, the size of cyberspace grows continuously. Small computers and microchips are installed everywhere; not only in the traditional information systems, but, for example, in furniture, clothes, means of payment, and weapon systems. It is not a question of processor power, but of the number of computers. These computers are not only installed separately, but they are also connected to the global network, Internet. In 2010, there were over 2.1 billion Internet users on Earth[6]. Nowadays, a connection to Internet is more important than the power of one's computer and it provides infinitely greater utility to the user. If computer users were isolated from one another, computer security management would be simple: concentrating on the personnel background checks and padlocks. However, the benefits of networking are too great to ignore, and modern organizations require Internet connectivity.[7] It is important to find a balance between functionality, performance and security.

Although the idea of a computer worm or virus was invented by mathematician John von Neumann in 1949, such malware remained in an experimental stage until the early 1990s.[8] In the 1970s and 1980s, hackers wrote viral programs, such as the Creeper worm, but these programs did not yet attempt to steal or destroy data.[9] During the 1990s, as the number of Internet users grew exponentially, there was an explosion of malware in both quantity and quality. When home computers began to emerge in the 1980s, hackers began to explore their potential and possibilities.[10]

The Estonian (2007) and Georgian (2008) conflicts were the first events in which cyber attacks were used to gain more effect on adversaries. Analysts say that the denial-of-service attacks in Estonia demonstrated a cyber attack model in which the critical services of an IT-dependent country are disturbed. The Georgian War demonstrated that there will be a close relationship between cyber and conventional operations in all future military campaigns.[11]

Until Stuxnet in 2009, the cyber incidents were more or less caused by hackers, activists or criminals – even in the cases of Estonia and Georgia. Stuxnet showed for the first time that a target can be hit without kinetic weapons and that a malware can be used to cause physical damages. The Stuxnet worm was designed to target industrial software and equipment.12 Stuxnet was the first known state-lead cyber attack with the motivation to stop Iran's nuclear enrichment facilities.13

Many countries have begun to put money and research into their cyberwarfare programs.[14] Cyber weapons have become the new tool of modern warfare. Stuxnet showed that cyberspace can be used to affect the physical world. An important strategic challenge for cyber defence is that Internet and information technologies change quickly. It is difficult for any organization to manage all of the latest developments. Attackers continue to spoil an ever increasing number of operating systems, applications, and communications protocols.

[6] World Factbook, 2011.
[7] Geers, 2011.
[8] Chen and Robert, 2004.
[9] Eichin & Rochlis, 1989.
[10] Geers, 2011.
[11] Geers, 2011.
[12] Phillips et al, 2011.
13 Sanger, 2012.
[14] Phillips et al, 2011.

Cyber defenders have too many technical environments to protect. Thus, the actors who want to protect their systems must have good intelligence, depth in defence, automated attack detection, response capabilities, and other means to detect and react to cyber attacks.[15] These actors include private companies, individuals, governments, and military forces.

From Information Security to Cyber Security

Cyber security development in Finland has followed the global trends over the past decades. From the 1970s, when the importance of security features in information systems began to increase due to the growing computing power, multiuser computer systems and shared file systems[16], information security has been a critical aspect in the information processing systems of the Finnish Government and the Defence Forces.

The latest crucial change in the area of information security threats has been the emergence of communication networks that have spread everywhere to connect computer systems worldwide. These networks also connect the governmental and defence sectors, and their computer systems. Internet protocols (IP/TCP) have become "de facto" standards. They have been cost-effective solutions for the security authorities and other critical service providers as well. The problem is that the protocols have been developed at a time when Internet was mostly used by researchers; when the overall number of users was relatively small; and when no hostile users appeared. Thus, the protocols originally did not include any security features, such as user or source address authentication.[17]

From the 1990s onwards, the rapid growth and the global use of computers and networks in data processing and electronic business, along with the increasing security threats (hackers, terrorists, criminals, and so on), fuelled the need for new methods to protect the computer and information systems.[18] During the 1990s, information security also became a serious business for the Finnish governmental and defence actors. In 1993, the Finnish Government made a policy decision[19] about government information security. The policy decision stated the responsibilities for information security, and introduced the basic elements to be considered when providing information security.

A new policy decision[20] replaced the previous one in 1999. The purpose of the new information security decision was to improve the security level of organizational information processing and personal data protection. The decision also provided recommendations for information security development and management. Moreover, the decision specified the information security responsibilities and the division of work, and identified the key information security tasks of different authorities. The decision stated that each authority must ensure that information security and data protection are realized in the authority's organization. The policy decision also emphasized that the government's information and data systems and services are the key functions forming the essential, economically valuable,

[15] Geers, 2011.
[16] Ritchie & Thompson, 2000.
[17] Abbate, 2000.
[18] de Leeuw & Bergstra, 2007.
[19] Valtioneuvoston periaatepäätös tietoturvallisuuden kehittämisestä valtionhallinnossa, 1993.
[20] Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta, 1999.

and nationally critical security information asset that requires high security for information and data networking.

At the beginning of the millennium, global business had become more and more dependent on computer networks and Internet. IP networks were spread all over the world. This development also applied to the Finnish society, which was already highly dependent on computer networks and services. The importance of information and network security was noticed by the Finnish Government. Thus, the Finnish Security and Defence Policy 2001[21] white paper stated that ensuring information security in information and networking systems had become part of the fight against terrorism. The policy paper also remarked that the development and integration of networks and information systems may have had unpredictable effects on information security. The paper recommended building separate networks that would provide an improved level of information security and reliability. The information security and warfare related responsibilities of the Defence Forces were described at a very abstract level. According to the paper, the Defence Forces had an important role in the development of defensive information warfare measures. The term cyber defence was not used at all.

The Finnish Security and Defence Policy of 2004[22] declared information warfare as an asymmetric threat. Asymmetric methods of warfare can be used to damage even a superior adversary. An open and highly developed information society is particularly vulnerable to asymmetric attacks. Security threats to information systems have multiplied, and an information society relying heavily on information networks and systems is vulnerable to malfunctions and crime. Attacks and attempted attacks on information systems occur daily, and the governmental communications and information systems are also under threat. The targets of information warfare include decision-makers, individuals, media, energy suppliers, information networks, and airspace management. In addition, the threats are similar to both civilians and the military.

As in the previous policy paper (2001), the Defence Forces had still an active role in the creation of the nationwide readiness for advance protection against information warfare threats. For the first time, the defence policy paper assigned an information warfare development task to the Defence Forces. According to the policy paper, information warfare capabilities had to be developed as an entity with the objective of setting up and introducing national operating methods that responded to the potential threats. Resources were to be concentrated on electronic and information systems warfare. The initial focus was on the continued development of defensive systems, and on the information attack method research. Later, the development has continued and expanded to cover also counter-measures capability.

The latest Finnish Security and Defence Policy[23], published in 2009, draws a threat scenario which consists of political and economic pressure and of various means of information warfare – including cyber attacks to disturb the normal functions of the society. Cyber defence and cyber security guidelines for the Defence Forces are limited to a few sentences: defence capabilities against an enemy's cyber attacks must be maintained and improved, and

[21] Finnish Security and Defence Policy 2001.
[22] Finnish Security and Defence Policy 2004.
[23] Finnish Security and Defence Policy 2009.

network-centric warfare must be taken into consideration in the ICT development of the military.

A growing interest in cyber security issues can also be found from the Finnish Government Program 2011[24] (the plan of action of the Government for its planned four year term). This program declares that the new security challenges, such as cyber attacks, require higher and more systematic readiness in the networked world. The reliability of information systems and networks is critical when operating in a modern information society. The main cyber security task in the program is the preparation of a national cyber strategy. The goal is that Finland becomes the leading country in the development of cyber security.

In the Finnish Defence Forces, cyber security has been part of military operations and planning since the first computers were introduced. Information protection was provided under the term information security until the 2010s. From the 1960s, the main actors on the information security field have been the Defence Command Operations Division, which has the main responsibility, and the Defence Forces C4 Agency (and its predecessors). The role of the C4 Agency is to build and maintain information services and networks. Security has always been a critical part of this task.[25]

During the 1990s and 2000s, information security in the Defence Forces included defensive measures to protect mission critical information. The requirements for information security were generated by the Defence Forces until information sharing with international partners (which is based on binding inter-governmental agreements) required new measures to be considered.

In 2008, the Ministry of Defence was set responsible for providing a common security auditing criterion (KATAKRI)[26] for authorities and private companies. The first KATAKRI version was completed in 2009, and the second version was published in 2011. The criterion is a tool that helps fulfilling international information security requirements. It also provides standardized practices for national level data security audits in the private sector.

By examining the development of cyber security over the past three decades, it can be said that the introduction of a new term, "cyber", has not changed the basic idea of the information and computer networks protection. What is new is that the integrated circuits, computers and communication networks have become an important part of the daily lives of businesses, individuals, the government and the military. Computers and networks, as well as their security, are therefore not only a business of the IT security geeks, but that of all citizens. Today, the physical world events and functions are connected to cyberspace events and functions. It is therefore valid to talk about the wider term, "cyber security", and not just about the information security of computers and networks.

[24] Programme of the Prime Minister Jyrki Katainen's Government, 2011.
[25] The Finnish Defence Forces Homepage, www.mil.fi.
[26] National Security Auditing Criteria, 2011.

The Current State

Today, the Government and the Defence Forces acknowledge the importance of cyber security. Most countries prepare for cyber threats, and larger proportions of budget have been allocated to cyber security related issues. Several national cyber strategies have already been published, while some are still under development. At the time of writing, the Finnish Government is also drafting a national cyber strategy. The task was launched in the previously mentioned government program 2011. The strategy should be published in the beginning of the year 2013. The responsibility for the preparation of the strategy lies with the Security and Defence Committee (TPAK), which operates under the authority of the Ministry of Defence. In practice, the strategy is written by a cross-administrative working group of experts.[27]

The purpose of the strategy is to provide cyber security guidelines to all relevant authorities. The first point is that all parties recognize the significant need for a change caused by the developments in the cyber domain. This requires new approaches, new thinking, and greater strategic agility. Finland already has an excellent starting point for that change as a small, dynamic country.[28]

The execution of the cyber security strategy also requires a 100 percent commitment to the common vision, strategy and procedures, which are conducted by following the policies and procedures of the Security Strategy for Society.[29] The current Security Strategy for Society includes cyber threats as one of the thirteen threat scenarios against functions vital to the society. Realization of cyber threats could cause serious disturbances in the telecommunications and information systems.

The cyber security strategy will provide a clear division of responsibilities and tasks between the ministries, businesses and industries. Strong cooperation is Finland's competitive advantage. The most concrete issue of the strategy is the establishment of a national cyber centre. The cyber centre will maintain situational awareness, improve coordination between actors, accelerate decision making, and develop cyber security related skills. This enables improved strategic sensitivity, flexible resource usage and consistency of management. In addition, Finland needs a cluster of cyber security companies to develop knowledge and technical solutions. The cluster is planned to work in close cooperation with the cyber centre.[30]

The current strategy work is a key driver on the strategic level. On the practical level, the most important governmental cyber actors are CERT-FI and NCSA-FI. CERT-FI is the Finnish national computer security incident response team with the main task of promoting security in the information society by preventing, observing, and solving information security incidents and disseminating information on threats[31]. Finnish telecommunications providers are the main customers and partners of CERT-FI. This is largely due to the operators' obligation (by law) to report all information security incidents to CERT-FI.

[27] Kansallista kyber-strategiaa valmisteleva työryhmä -hanke, 2011.
[28] Programme of the Prime Minister Jyrki Katainen's Government, 2011.
[29] Security Strategy for Society, 2010.
[30] Kosonen, 2012.
[31] CERT-FI Homepage, www.cert.fi.

According to the Finnish law, all identified threats to information security must also be reported.

NCSA-FI is a national communications security authority that specializes in information assurance matters related to the handling of classified information in electronic communications. It is part of Finland's security authority (NSA) organization. At the international level, NCSA-FI duties include: guidance related to the handling of international classified information, management of the crypto material and its distribution network, approval of cryptographic products, accreditation of information systems processing international classified information, and responsibility for national TEMPEST activities[32].

In Finland, the central government's information security policy and information security guidance matters are the responsibility of the Government Information Security Management Board (VAHTI), which operates under the authority of the Ministry of Finance. VAHTI has an important role in cyber security, since it is responsible for steering, developing and coordinating the central government's information security. The administrative branches allocate budget funds and other resources to the development of information security and cooperation based on the guidance of VAHTI. Through cooperation, preparation and coordination VAHTI develops the central government's cyber security and data protection, and promotes good operating practices in the cyber security work of the public administration.[33]

In the Defence Forces, cyber defence is understood as the national defence part of cyber security[34]. Cyber defence is an operational capability in cyberspace and hence similar to the capabilities of the Army, Air Force and Navy. Cyber defence consists of defensive, offensive and intelligence capabilities. Cyber defence capabilities are used within the law. At the time of writing, the Defence Forces are preparing their own cyber concept which will include the description of the role of the military forces in cyber defence, and guidance in cyber capability development[35]. The role of the Defence Forces will be based on the jurisdiction designated to the military.

Cyber capabilities are not developed at the expense of land, air and/or maritime warfare capabilities. Currently, it is estimated that in the foreseeable future a pure cyberwar in which no other traditional capabilities are needed will not take place. Cyber attacks are not yet enough to compensate for the effects of traditional attacks. For a small technologically developed country, such as Finland, cyber defence is a cost-effective opportunity to strengthen her defence capabilities. Some resources are obviously needed for the development and maintenance of cyber capabilities, but their costs are lower than what the traditional weapons require, as the most important asset is human knowledge.[36]

In October 2011, the Finnish Ministry of Defence announced that the Defence Forces also develop offensive cyber weapons[37]. Building up an effective cyber defence requires the ability to use offensive weapons and, in some cases, cyber attacking is the best defence. The

[32] NCSA-FI Homepage, www.ncsa.fi.
[33] Valtioneuvoston periaatepäätös tietoturvallisuuden kehittämisestä valtionhallinnossa, 1993.
[34] Muuriankkuri, kesä 2012.
[35] Ruotuväki, n:o 15/2011.
[36] Maanpuolustus, 4/2011.
[37] Helsingin Sanomat, 12.10.2011.

representatives of the Defence Forces announced, firstly, that the development of offensive weapons is expectable and, secondly, that it is what the superpowers and other countries carry out when preparing for cyberwarfare.

The organizational preparations for cyber defence started in summer 2011, when the Cyber Defence Sector of Defence Command C4 Division was established to manage and control the development of cyber capabilities throughout the Defence Forces[38]. Last organizational changes took place at the beginning of 2012, when the organization of the Defence Forces C4 Agency was modified to fit better to the cyber defence challenges[39]. The Defence Forces have already started to recruit the first professionals[40]. Whereas the land, sea and air forces improve their readiness when the threat of crisis grows, cyber defence requires continuous readiness and thus, appropriate personnel recourse is a critical issue. In addition, the Defence Forces has an ongoing cyberwarfare program to build up cyber defence capabilities[41]. Simultaneously, cyber defence situational awareness and understanding are developed, and cyber defence research and education are participated.

Today, international cooperation is an important part of cyber defence development. Cooperative partners are naturally the same with whom Finland has worked for the past years. In the area of cyber defence, the main international partners are NATO and the Nordic countries. NATO has stated that because cyber threats do not recognize geographical and organizational borders, cooperation with partners in cyber defence is significant[42]. Finland, as a NATO partner, has participated in some NATO cyber security working group meetings. In addition, cooperation with NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) has already begun. Finland's contribution is implemented through the Partnership for Peace program.[43]

Collaboration related to cyber security also takes place under the umbrella of the Nordic Defence Cooperation (NORDEFCO). The latest discussion on the potential for cyber security collaboration was conducted in the Nordic foreign ministers' meeting in October 2012. The Nordic governments have identified cyber as a vital area for urgent cooperation. The common capabilities include, for example, joint countermeasures, plans and strategies. These capabilities should be established between 2014 and 2015. The common Nordic expertise will involve dedicated national military cyber defence centres working closely with the private sector. The first step in implementing the cyber initiative will be the creation of interconnected networks to link national cyber centres and regulatory authorities.[44]

Cyber security and cyber defence are very common terms in the contemporary debate attended by politicians and/or military leaders which depicts the importance and the role of cyberspace. It seems that cyber security threats are taken seriously, and that the leaders are willing to provide resources to improve cyber security. The ongoing preparation of the Finnish national cyber security strategy shows that the state leaders desire to prepare for cyber threats. A good example of the practical actions taken is the preparations conducted for

[38] Muuriankkuri, kesä 2012.
[39] Verkostopuolustus, syksy 2011.
[40] YLE Uutiset, 29.10.2011.
[41] Verkostopuolustus, syksy 2011.
[42] NATO and cyber defence, www.nato.int.
[43] Defense News, 20.10.2011.
[44] Defense News, 2.11.2012.

establishing the new national cyber centre for coordination and guidance in cyber security related issues, and for maintaining a national cyber situational picture.

Today, one of the main problems with cyber security is its fragmentation within the public administration[45]. Each administrative branch is responsible for the security of its own systems. Information and cyber security responsibilities have been shared among too many actors. None of the actors has the overall responsibility – or the overall situational awareness. With a growing number of cyber threats, the situation should be clarified. The national cyber centre proposed by the strategy will help with the situation in the near future. Situational awareness is a global challenge for both military and civilian actors. The situational awareness systems should be built so that they could monitor and detect cyberspace events on the appropriate level. Anomalous situations should be recognized somehow in order to prevent damages in the cyber domain.

In the military cyber defence, one of the challenges is offensive capabilities. It is not only a question of the types of weapon, but also of a military doctrine. Cyber weapons are new tools to affect adversaries, even over the borders, and they are easy to use already in peacetime. The use of the weapons should be clearly defined, and the best way to do that is to publish a public cyber doctrine. Moreover, the international laws are not yet that clear about cyber weapons, their targets and permissible effects. With regard to cyber weapons, it is also challenging to achieve the desired effect on the target without any unexpected side effects. As information systems and networks are complexly dependent on each other, a cyber event in one spot of the network could suddenly affect another point in the network and cause something unpredictable. Another challenge relates to reacting to cyber attacks. Disconnecting communication links or closing information services are not relevant alternatives anymore. Thus, it is a question of when and how to use cyber or traditional forces against the attacker. An updated military doctrine could help in this situation.[46]

Although the military budget in Finland has been cut, the military officials are still eager to allocate resources to the development of cyber defence47. The Finnish Defence Forces have been quite calm with the beginning of the construction of cyber capabilities and, for example, a separate cyber command has not yet been established – unlike in some other countries. The United States, which is a leading country in cyber defence, has already established the United States Cyber Command that is a sub-unified command subordinate to the US Strategic Command48. It is obvious that smaller countries cannot put that many resources into cyber defence and thus, it is difficult to say whether the current resources are enough in relation to the threat level.

Future Trends of Cyber Security

The Government Program states that the goal of Finland is to become the leading country in the development of cyber security[49]. The strategy preparation working group has published

[45] Signaali, 4/2011.
[46] Kylkirauta, 1/2012.
[47] Defense News, 20.10.2011.
[48] www.stratcom.mil/factsheets/cyber_command/.
[49] Programme of the Prime Minister Jyrki Katainen's Government, 2011.

a vision according to which Finland is a world-wide pioneer in preparing for cyber threats and incident management in 2016[50]. The vision may sound optimistic, but the people behind it believe that Finland has good chances to reach the goal. Since the wars of the 1940s, preparedness and the security of supply have been a common issue for the entire Finnish society, and Finland already has the political forums that could also coordinate the development and management of cyber security. Cooperation between different authorities is already a well-established practice. Finland is a compact and small enough country to make things comprehensively at the national level within a reasonable period of time. Finland also has expertise in technical cyber security solutions for both domestic needs and export.

The cyber strategy will confirm the role of the Finnish Defence Forces in the area of cyber security. In the future, cyber capabilities of the Defence Forces will be developed for military operations, and they will be used mainly as a part of the military force. Defensive cyber capabilities will be required to protect the infrastructure of the Defence Forces already in peacetime. Under normal circumstances, the police and others security authorities will be responsible for protecting the society against cyber threats. However, in exceptional circumstances the role of the Defence Forces will increase due to offensive cyber operations and in coordinating the protection. The resources of the military are not enough to protect all critical information services and networks. Therefore, the resources and knowledge of other agencies, telecom operators and private companies will be essential for the protection.

Cyber defence will increase its importance in the near future.[51] Thus, it would be natural that the Finnish Defence Forces also increases its investment in cyber defence capabilities. However, it is difficult to predict how the status of cyber defence will change. A few countries have already raised their cyber defence to a high level. For example, the United States Cyber Command is a subordinate unified command under one of the combatant commands, USSRTATCOM.[52] Upcoming years will show, if a separated command is established also in Finland.

The development of cyberwarfare capabilities requires adequate legislation. National legislation must allow the development of both offensive and defensive cyber capabilities. Because the cyber playground is global, intense development of the international legislation is needed. Relevant questions are: what is the law of cyberwar, and how does the current Geneva Convention apply in cyberspace? Cyber weapons may be juxtaposed with conventional weapons, but there are still aspects that make cyber weapons different. For example, separating military and civilian targets could be difficult in cyberspace – as identifying the attacker would be. Thus, a new type of thinking is needed when developing a framework for international cyber security law.

International law is also required for the development of new cyber weapons. After the production of defensive security protection software and devices, it seems that the private business market will continue with the production of offensive cyber tools.[53] The development of offensive cyber weapons will become more aggressive and publicly more acceptable. First steps towards this direction have already been taken[54].

[50] Kosonen, 2012.
[51] Möckli, 2012.
[52] www.stratcom.mil/factsheets/cyber_command/
[53] "Stonesoft to Host First Cyber Security Summit in New York City…", 2012.
[54] Vupen Security Homepage, www.vupen.com.

Private companies are seen as part of the national and international network of cyber actors. The other actors include both civilian and military authorities. In Finland, the national cyber centre will play a major role in coordinating and controlling cyber actors. In addition, different volunteer based non-profit organizations are important for the national cyber defence as they provide innovation on and knowledge of different cyber security areas. If these resources are wanted for national/governmental use, the organizations need appropriate forums and procedures to act and communicate.

Cyberspace is changing military strategies and doctrines, because it possesses many features that even the great theorist of war, Sun Tzu, could not have imagined in the ancient China. The rapid production of cyber weapons, tools and tactics makes it impossible for any nation or organization to be familiar with all of those weapons and the associated threats. The cyber battlefield does not have geographical borders, and cyber events occur at the speed of light. Cyber attacks can be executed with such a high degree of anonymity that traditional defence strategies, such as deterrence and retaliation, are no longer credible.[55]

Therefore, many governments may conclude that, for the foreseeable future, the best cyber defence is a good offense. First, cyber attacks may be required to defend the homeland; second, they are a powerful and sometimes deniable way to project national power.[56]

A national situational picture of cyber security events will be a critical entity. A common picture would help the coordination of incident handling, and it could also provide some ability to predict cyber events. Information sharing requires trusted communication systems. Therefore, the question is who coordinates the building of such information sharing system – and where do the required resources come from.

Knowledge of cyber operators is a significant capability in military cyber defence. In many cases, the level of cyber defence correlates with the skills of an individual operator. Cyber weapon systems may cost a lot less than the expensive traditional weapon systems, because their effectiveness is based on the knowledge of the cyber operators. It could be just enough for conducting cyber operations to have a group of people with high-level skills and access to networks. Personal knowledge and skills are important issues that countries will compete for in the near future. Although simple cyber attacking may not require major resources, specific simulation and test environments could cost a lot. In the future, military planners must be able to simulate cyber attacks and test cyber defence in a safe laboratory environment which does not influence the operational networks[57].

International cooperation will strengthen the cyber capabilities of Finland also in the future. NATO and the Nordic cooperation will provide more knowledge and cost-effectiveness in cyber defence matters. Developing the Nordic cooperation will increase its significance in cyber security. The cyber domain enables light and easy-prepared training. In the following years, cyber actors should develop the cyber training process towards the Over Border training system which is already used between the Air Forces of the Nordic countries. Building up a cyber training network could be one of the key goals for the upcoming years.

[55] Geers, 2011.
[56] Geers, 2011.
[57] Geers, 2011.

Cyber defence is an important element in the revised NATO policy[58]. NATO states that as cyber threats do not recognize state borders and organizational boundaries, cooperation with partners is critical. NATO will be an important partner to Finland. NATO is still the leading organization in standardization and military capability development. NATO's cyber capabilities and knowledge will increase in the future. However, as a partner Finland will receive only limited information about cyber threats, technologies, and lesson learned. A military alliance could possibly bring more resources for conducting cyber operations. The knowledge and technology from the alliance members could improve significantly the national ability to defensive cyber operations. Instead, the challenge could be to get support for cyber intelligence and offensive operations, which are still quite sensitive areas. The challenge could remain even through the interpretation of the Article 5.[59]

Future military doctrines have to address the use and development of cyber weapons. The new weapon system allows the use of new operational principles, targets and effects. In the new doctrines, cyber weapon should also be seen as internally asymmetric[60]. Military planners should think how to affect an adversary's cyber weapon even before attacking. Focusing only on stopping attacks may not be enough, because the attacks could include zero-day vulnerabilities that are not even known.

The Finnish cyber defence strategy should be public. It would describe the operating principles of the established cyber defence. The public cyber defence strategy would act as a deterrent and steer the national development. It would also facilitate the citizens' understanding of the use of cyber weapons and its role in the national defence. In addition, the doctrine would define how and in what circumstances cyber attacks are responded. Moreover, it would state when our own cyber weapons are used. The national defence in Finland is based on a large reserve. In the future, the Defence Forces should solve how to use reservists in cyber defence tasks. Due to the large number of internationally known cyber security companies in Finland, the Defence Forces' reserve has high-skills and plenty of knowledge relevant to military tasks in store. This would also add a significant resource to cyber defence.

Conclusion

The Finnish Government and the Defence Forces proclaim that cyber security and cyber defence are very important issues. Cyber threats are serious and existing. These threats are among the most crucial ones with regard to the Finnish society. It is not merely a question of protecting and defending information since the entire information processing infrastructure keeps the economic, political and social ecosystems running.

It is also noticed that the threat is not bypassing. While individuals, organizations and business are more and more networked, information systems and communication networks become more complex. This complexity creates new cyber threats and attacking surfaces. It is very difficult to see that the threats will be smaller in the future.

[58] "Defending the networks", 2011.
[59] Sirén, 2011.
[60] Kylkirauta, 2/2012.

The Government and the Defence Forces have begun to allocate resources for cyber security capabilities. The ongoing cyber security strategy work and the latest organizational changes indicate this development. However, if we consider the global development lead by the United States, we immediately notice that the current resources may not be enough. In addition to money, cyber security requires legislation, coordination, cooperation and appropriate communication channels between the authorities.

The upcoming cyber strategy will guide the Finnish cyber security development for the next decade. Thus, the strategy will play an important role also in the development of cyber defence in the armed forces. The tasks and responsibilities defined in the strategy will help the Defence Forces to focus on the right development spots.

Cyber defence, originally transformed from information security, has become a strategic-level issue. Some years ago, information security was only an issue for system operators and maintenance personnel. Security problems and challenges were solved by engineers. Currently, cyber security touches upon every organization's and each individual's daily life. Protection against threats requires strategic-level decisions, because cyber defence not only depends on the security technologies, but also on strategic guidance and coordination, as well as on resource allocation. Cyber security concerns all organizations utilizing information services and networks.

If we look at the history of information and cyber security in Finland, we see that the Government and the Defence Forces have tried to provide the necessary means to protect the critical information environments. Information and cyber security have not been major drivers in the Government's acts until the past few years. The allocated resources and the speed of the development have not been at the same level as in the leading countries, such as the United States. However, the cyber challenges and threats are now focused on with a delay. Currently, it seems that the threat is acknowledged and reacted on, and that the direction of the development is correct. The contemporary challenge is to decide how cyber security and defence will be implemented in practice.

References

”Armeija palkkaa väkeä kybertaisteluihin”, YLE Uutiset, 29.10.2011, http://yle.fi/uutiset/armeija_palkkaa_vakea_kybertaisteluihin/5444616. [cited 8.11.2012]

C. Candolin, ”Kyberpuolustus – uusi maanpuolustuksellinen ulottuvuus,” Kylkirauta, Maanpuolustuksen ja johtamisen erikoislehti, n:o 1, 2012.

CERT-FI Homepage, www.cert.fi. [cited 8.11.2012.]

Chen, T. and Robert, J-M. (2004) “The Evolution of Viruses and Worms,” Statistical Methods in Computer Security, William W.S. Chen (Ed), (NY: CRC Press) Ch.16, 265–286.

"Cyber Defense Takes Center Stage in Nordic Cooperation", Defense News, 2.11.2012, http://www.defensenews.com/article/20121102/DEFREG01/311020001/Cyber-Defense-Takes-Center-Stage-Nordic-Cooperation. [cited 8.11.2012]

Cyber Warfare - Understanding the Threat to Weapon Systems, The WSTIAC Quarterly Report, Volume 9, Number 4, 2009.

D. E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," New York Times, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html [cited 15.11.2012]

D. Möckli, Strategic Trends 2012: Key Developments in Global Affairs, Center for Security Studies, ETH Zurich, 2012.

Defending the networks, The NATO Policy on Cyber Defence, NATO Public Diplomacy Division, NATO, 2011.

Eichin M.W. & Rochlis, J.A. (1989) "With Microscope and Tweezers: an Analysis of the Internet Virus of November 1988," IEEE Computer Society Symposium on Security and Privacy 326–343.

"Finland To Develop Cyber Defense 'Counterpunch'", Defense News, 20.10.2011, http://www.defensenews.com/article/20111020/DEFSECT04/110200306/Finland-Develop-Cyber-Defense-Counterpunch-. [cited 8.11.2012]

Finnish Security and Defence Policy 2001, Report by the Government to Parliament, (ISBN 951-53-2328-2), 13.6.2001.

Finnish Security and Defence Policy 2004, Government report 6/2004, Prime Minister's Office: Publications 18/2004, Edita 2004.

Finnish Security and Defence Policy 2009, Government Report, Prime Minister's Office Publications 13/2009, 5.2.2009, Helsinki University Print, 2009.

H. Ohra-aho, pääkirjoitus, Verkostopuolustus, Puolustusvoimien johtamisjärjestelmäkeskuksen sidosryhmälehti, syksy 2011.

http://www.stratcom.mil/factsheets/cyber_command/ [cited 8.11.2012]

Instructions on Implementing the Decree on Information Security in Central Government, The Government Information Security Management Board (VAHTI), Ministry of Finance Finland, 2b/2010, Tampereen Yliopistopaino Oy, 2012.

J. Abbate, Inventing the Internet, MIT Press, 2000.

J. Andress and S. Winterfeld, Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, Elsevier Inc, 2011.

”Kansallinen kyberturvallisuusstrategia etenee”, Signaali, Viestintäviraston asiakaslehti, n:o 4, 2011.

K. de Leeuw, and J. Bergstra (ed.), The History of Information Security: A Comprehensive Handbook, Elsevier, 2007.

K. Geers, Strategic Cyber Security, CCD COE Publications, July 2011

Kansallista kyber-strategiaa valmisteleva työryhmä -hanke (PLM001:00/2011), hankerekisteri, http://www.hare.vn.fi/mHankePerusSelaus.asp?h_iId=17515. [cited 14.11.2012]

”Kyberpuolustus osana maanpuolustusta”, Muuriankkuri, Puolustushallinnon Rakennuslaitoksen sidosryhmälehti, kesä 2012.

M. Hyytiäinen, ”Ajatuksia Kybersodankäynnistä”, Kylkirauta, Maanpuolustuksen ja johtamisen erikoislehti, n:o 2, 2012.

M. Kosonen, Yhteiskunnan turvallisuusfoorumi 28.9.2012. http://www.lahdenmessut.fi/material/kosonen_yhteiskunnan_turvallisuusfoorumi_280912.pdf

Moore’s Law, Intel Corporation, www.intel.com/technology/mooreslaw. [cited 15.11.2012]

N. Phillips, C. Wright and J. Troop, United Nations Security Council: Cyber Warfare, Report, March 26th, 2011.

National Security Auditing Criteria (KATAKRI), National Security Authority, version II, 2011.

NATO and cyber defence, http://www.nato.int/cps/en/natolive/topics_78170.htm. [cited 8.11.2012]

NCSA-FI Homepage, www.ncsa.fi. [cited 8.11.2012]

Programme of Prime Minister Jyrki Katainen’s Government, Prime Minister’s Office, Finland, 22 June 2011.

R. F. Bellaver, Characters of the Information and Communication Industry, Author House, 2006.

Ritchie, D. and Thompson, K., The UNIX time-sharing system, Communications of the ACM, Vol. 17, Issue 7, s. 365–375, July, 1974.

Security Strategy for Society, Government Resolution, Ministry of Defence, 6.12.2010.

Stonesoft to Host First Cyber Security Summit in New York City, Press Release, September 25, 2012, http://www.stonesoft.com/us/press_and_media/releases/us_english/2012/25092012.html. [cited 12.11.2012]

”Suomesta luodaan kyberasioiden edelläkävijää”, Ruotuväki, Puolustusvoimien uutislehti, n:o 15/2011, 25.8.2011.

”Suomi valmistautuu kybersodankäyntiin”, Helsingin Sanomat, 12.10.2011.

T. Sirén (toim.), Strateginen kommunikaatio ja informattio-operaatiot 2030, Article Collections N:o 7, Department of Leadership and Military Pedagogy, National Defence University, Helsinki 2011.

The Finnish Defence Forces Homepage, www.mil.fi. [cited 8.11.2012]

Valtioneuvoston periaatepäätös tietoturvallisuuden kehittämisestä valtionhallinnossa, Valtiovarainministeriö, VM 1/73/93, 4.2.1993.

Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta, Valtiovarainministeriö, VM 0024:00/02/99/1998, 11.11.1999.

Vupen Security Homepage, http://www.vupen.com/english/services/lea-index.php. [cited 12.11.2012]

World Factbook 2011, Central Intelligence Agency, 2012.

Y. Benson, ”Kansallinen kyberturvallisuus”, Maanpuolustus, n:o 98, 4/2011.

Norwegian Cyber Security: How to Build a Resilient Cyber Society in a Small Nation

Kristin Hemmer Mørkestøl[1]

Abstract

The article provides an insight into the Norwegian process towards increased robustness in cyberspace. The aim is to share lessons learnt which may be of use for other smaller nations facing similar endeavours, such as raising awareness on the need to clarify cyber roles and responsibilities within government, as well as the importance of cyber competence amongst decision makers. The article also challenges the reader on cyber issues of national and international relevance that deserve further exploration, such as the application of international law and the use of worst-case scenarios for better preparedness planning in the cyber domain.

Keywords: Norway, cyberspace, cyber security, cyber defence, resilience, decision makers, preparedness

Introduction

In Norway's quest for enhanced resilience in cyberspace we have both encountered challenges and achieved results that may be of interest to other small nations. In this article, I first describe the important steps Norway has taken towards increased robustness in our national information and communication systems. I then address some of the challenges encountered in the endeavour, as well as some of the lessons learned. Finally, I point to some issues that should be further explored in time to come, both nationally and internationally.

This article will not cover details about the threats in cyberspace. Instead, it will focus on measures taken to address the challenges those threats pose. Due to the nature of the threats, I primarily address the strategic (and to some extent the operational) civil-military aspects of these measures, rather than the military or civilian tasks alone.

Cyber Defence in Norway

Norway has a long history of civil-military cooperation. This cooperation is known as the "total defence concept". The same concept forms the basis of Norway's approach to the challenges in cyberspace.

[1] The opinions expressed in this chapter are those of the author, and should not be considered as the official policy of the Norwegian government.

The Norwegian Total Defence Concept and Its Relevance for Cyber Defence

The concept of Total Defence ("Totalforsvaret") was coined in Norway in the aftermaths of the Second World War. The Defence Commission of 1946 underlined that the defence of Norway would need to be built on both military defence and broad civilian preparedness. The aim of this approach was to secure Norway's territory, independence and national values, and to safeguard the population.[2] The concept responded to a need for ensuring a comprehensive effort by all sectors in the society in times of crisis, and for avoiding unnecessary duplication of effort in a small nation like Norway.

The concept is still relevant in Norway, although as a modernised version. From 1946 onwards, the focus was primarily on securing civilian support to military defence in war or warlike situations. In 2004, the government of Norway decided to modernise the concept and broaden its scope. This modernisation ensured the relevance of the concept not only for war, but also for crises in peace.[3] Today, the total defence concept implies mutual support and cooperation between the armed forces and the civilian society along the full spectrum of challenging situations – from a crisis in peace to a security policy crisis and an armed conflict.[4]

Both the civilian and the military sector live and work in cyberspace. Much of our civilian information infrastructure is to be considered national critical infrastructure. Over the years, we have seen how both civilian and military sectors worldwide are being targeted by actors in cyberspace seeking to disrupt, deny, deceive, degrade, destroy or in any other way affect computer networks and other communication infrastructure (including SCADAs[5] etcetera). As the victims of such offences may be both civilian and military, response measures need to be implemented in both of these sectors. The Norwegian crisis management and preparedness planning is governed by the "principle of responsibility".[6] This means that every sector is responsible for managing crises within its own sector – including cyber attacks. For Norway, the total defence concept implies mutual support and cooperation between the military actors responsible for cyber related tasks and the civilian actors in the same domain – in peacetime crises as well as in armed conflicts.

---

[2] Forsvarskommisjonen av 1946 (1946), part 3, page 5.

[3] St.prp. nr. 42 (2003-2004) «Den videre moderniseringen av Forsvaret i perioden 2005-2008» (2004), boks 5.2, and «Innstilling fra forsvarskomiteen om den videre moderniseringen av Forsvaret i perioden 2005-2008», Innst. S. nr. 234 (2003-2004) (2004).

[4] Forsvarsdepartementet, Støtte og samarbeid. Det moderniserte totalforsvarskonseptet – en oversikt over viktige ordninger og retningslinjer (2007), pages 10–11.

[5] SCADA: Supervisory Control and Data Acquisition system (software programs).

[6] The "principle of responsibility" is one of three important principles in Norwegian crisis management and preparedness planning, the other two being the principle of similarity (the organisation managing a crisis should be similar to the organisation normally responsible for managing the subject) and the principle of proximity (the crisis will be handled at the lowest possible level. Security policy crisis and nuclear incidents are exempt from the principle of proximity as they will always be handled at strategic level). Forsvarsdepartmentet, Støtte og samarbeid. Det moderniserte totalforsvarskonseptet – en oversikt over viktige ordninger og retningslinjer (2007), page 18.

Norwegian Cyber Defence and the Lessons Learned

Norwegian cyber security has developed steadily over the past decade. A number of challenges have been encountered, especially, when creating the superstructure for cyber defence, that is, the structure at the strategic level. Our lessons learned may be of value for other states working their way along the same path.

Norwegian Cyber Defence: Operational Cooperation and National Strategies

In 2000, the Norwegian Early Warning System for Digital Infrastructure ("Varslingssystem for Digital Infrastruktur", VDI) was established. The VDI was initially a project developed between the Norwegian intelligence and security services, and it was the first national system for penetration detection in the world based on cooperation between public and private actors.[7] In 2003, the VDI was moved under the then newly established National Security Authority and it gained the status of a permanent system. The VDI was an early nucleus of the national Computer Emergency Response Team (CERT).[8] When the Norwegian CERT (NorCERT) was formally established within the National Security Authority in January 2006, the VDI became an integral part of it.

NorCERT is a national service, serving both public and private actors in all sectors of the society. NorCERT is responsible for coordinating the management of cyber defence measures in case of cyber attacks in Norway. The NorCERT structure includes an operational centre, an analysis and information sharing section, as well as the VDI. The VDI is based on membership. The members are actors in all sectors of the society (public services, defence, energy, bank and finance institutions, as well as gas companies and more). Several of them are responsible for critical functions in Norway. These members take part in the VDI sensor system. Data collected from the sensors are voluntarily handed over to NorCERT, where the data may be analysed in order to identify cyber attacks. If a cyber attack is detected (through the sensors), the relevant members of the VDI will be alerted in order for them to take action to protect their own systems. The cooperation taking place within the VDI is based upon openness and trust between the VDI and the members. Detailed information, such as information on a member's security measures and hostile activity in his or her networks, is confidential information and hence it is not shared by the VDI to the other members of the community.[9]

The main benefits for the members from such cooperation are that they may be warned when the VDI identifies cyber attacks against one or several actors in the VDI; they receive assistance in assessing the risk and analysing the threat; they are part of an information sharing environment; and they can participate in exercises.

---

[7] Nasjonal Sikkerhetsmyndighet (National Security Authority) homepage (accessed January 8th 2013): https://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/Internettsikkerhet---NorCERT/VDI/. See also text about VDI in the briefing "Virtual warfare" in von Rosenbach's article in Jane´s Defence Weekly, November 16th 2011 (2011).

[8] In some countries labelled "Computer (Security) Incident Response Team" (C(S)IRT).

[9] Nasjonal Sikkerhetsmyndighet (National Security Authority) homepage (accessed January 8th 2013): https://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/Internettsikkerhet---NorCERT/VDI/

Parallel to this development, various sectors have already developed their own cyber defence organisations, including the early warning systems. There is a "CERT"-like function in the Norwegian Armed Forces Cyber Defence (NOR CYDEF), as well as in the health sector[10] and in the universities[11] – and more of these are in the making.

A "joint cyber task force" ("Koordineringsgruppen for IKT risikobildet") was created in 2009 in order to ensure increased situational awareness. This task force is responsible for establishing and maintaining the national cross-sector information and communication threat picture. It consists of the three national intelligence and security services, that is, the Norwegian Intelligence Service, the Norwegian Police Security Service, and the National Security Authority. The task force ensures timely information sharing and coordination, both regularly and upon request.[12]

The Strategic Structure

The process of developing a cyber defence structure at the ministerial level matured as the VDI, NorCERT and cyber task force were established.

The first relevant national strategy dates back to 2003 ("National Strategy for Information Security").[13] The strategy was developed jointly by the Ministry of Justice, the Ministry of Defence and the Ministry of Trade and Industry in order to capture the comprehensive nature of the information environment. In 2007, the "Guidelines for Strengthening Information Security" were published, following up on the strategy from 2003.[14] The focus of these first documents was, first and foremost, directed towards information security. Securing information and communication infrastructure critical to the society was a prioritized area. The government also created a coordinating committee for preventive information security ("Koordineringsutvalget for forebyggende informasjonssikkerhet", KIS) in 2004. The KIS consists of representatives from ministries and directorates with a relevant responsibility within information security.[15]

In order to create a common understanding of the threats Norway will face in years to come, to identify areas of priority for the government, as well as to provide guidance for the roles and responsibilities, the government launched a revised version of the national strategy in late 2012 ("National Strategy for Information Security").[16] This version was followed by an action plan for implementation.[17] The areas of the highest priority for the government

[10] The CSIRT for the health sector under development, as decided by Parliament in Innst. 11 S 2010–2011 (2010), proposed by the Ministry of Health in Prop. 1 S 2010–2011 (2010), chapter 781.
[11] For instance the University of Oslo CERT.
[12] Koordineringsgruppen for IKT risikobildet: Bakgrunnsnotat Cybersikkerhet (2010), page 20.
[13] Forsvarsdepartementet et al., Nasjonal strategi for informasjonssikkerhet 2003-2007 (2003), signed by the ministers of Defence, Trade and Industry as well as Justice.
[14] The Guidelines were signed by the Ministers of Government Administration, Justice, Transportation and Defence. Fornyings- og administrasjonsdepartementet et al., Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007-2010 (2007).
[15] For more information see https://www.nsm.stat.no/Om-NSM/Samarbeidspartnere/KIS/.
[16] Fornyings- og administrasjonsdepartementet et al., Nasjonal strategi for informasjonssikkerhet (2012), http://www.regjeringen.no/nb/dep/fad/dok/rapporter_planer/planer/2012/nasjonal-strategi-for-informasjonssikker.html?id=710469 (accessed January 8th 2013), by the Ministers of Government Administration, Justice, Transportation and Defence.
[17] Fornyings- og administrasjonsdepartementet et al., Nasjonal strategi for informasjonssikkerhet Handlingsplan (2012), http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Handlingsplan_nasjonal_strategi_informasjonssikkerhet.pdf (accessed January 9th 2013).

within the field of information security were defined as 1) increased coordination and common situational awareness, 2) robust information and communication infrastructure in the society at large, 3) strong ability to manage undesired cyber activity, and 4) high level of competence and security awareness.[18]

Lessons Identified – and Learned

As depicted above, the government and the different sectors have been working steadily to increase cyber defence in the society at large. In this process, the actors were faced with several challenges.

One of the challenges was the question of placing responsibilities for cyber defence in the Norwegian government, as cyber threats by nature cut across different sectors. In countries such as the UK and France, cross-government institutions, such as the cabinet office, are often preferred for coordinating cyber defence. In the Netherlands, the coordinating responsibility is given to the Ministry of Security and Justice. In Norway, the organisation of the government[19], as well as the formerly mentioned principle of responsibility, imply that all Ministers are responsible for their own sector – also in the realm of cyber defence. On the other hand, the Ministry of Justice and Public Security is responsible for coordinating civilian crisis management and preparedness planning, while the Ministry of Government Administration is responsible for the development of information and communication technology policies. Both areas are important elements in cyber defence, but often cyber defence tasks are not easily divided into these two areas of responsibility. An example of an area not easily attributable to either the Ministry of Justice *or* Administration is communication tools for crisis management: should these be the responsibility of the Ministry of Justice or Administration? Such tools are relevant for preparedness planning and crisis management (Justice), and they are also a part of the general government's administrative tools and policy (Administration). Such "grey-zones" proved important to clarify.

The revised strategy (2012) is also useful for clarifying the roles and responsibilities in areas not easily attributable to only one sector. The Ministry of Justice and Public Security was given additional tasks and it will, according to the strategy, take over and develop the responsibility for information and communication security in the civil society at large.[20] This also implies that the Ministry of Justice will be responsible for ensuring the implementation of the National Strategy for Information Security.

In addition to this clarifying principle, the action plan[21] addresses the various tasks to be performed and identifies the responsible ministry/ies for each task. For example, the

[18] Fornyings- og administrasjonsdepartementet et al., Nasjonal strategi for informasjonssikkerhet (2012), http://www.regjeringen.no/nb/dep/fad/dok/rapporter_planer/planer/2012/nasjonal-strategi-for-informasjonssikker.html?id=710469 (accessed January 8th 2013), page 17.

[19] For a discussion on Norway's organisational structure with regards to ministerial responsibilities, see for instance Sårbarhetsutvalget, NOU 2000:24 Et sårbart samfunn, chapter 23, pages 263-274.

[20] Fornyings- og administrasjonsdepartementet et al., Nasjonal strategi for informasjonssikkerhet (2012), http://www.regjeringen.no/nb/dep/fad/dok/rapporter_planer/planer/2012/nasjonal-strategi-for-informasjonssikker.html?id=710469 (accessed January 8th 2013), page 15.

[21] Fornyings- og administrasjonsdepartementet et al., Nasjonal strategi for informasjonssikkerhet Handlingsplan (2012), http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Handlingsplan_nasjonal_strategi_informasjonssikkerhet.pdf (accessed January 9th 2013).

responsibility for communication tools for crisis management is given to the Ministry of Justice and Public Security, in cooperation with the Ministry of Defence.[22] As this action plan will be subject to revision from time to time, it may prove to be a useful tool in attributing responsibilities for future tasks.

Another important challenge in the quest for enhanced cyber security turned out to be knowledge. While several doctoral degrees have been conferred on advanced technological topics, little has come out with respect to the security policy implications of severe cyber challenges. This may in part explain why not all bureaucrats or decision-makers are well versed in the cyber domain. In addition, over the years the various sectors have developed their own specific terminology for different aspects of cyber challenges. The lack of agreed language led to discussions conducted on different levels, which caused frustration and misunderstandings.[23] In the Norwegian experience, several meetings were conducted between ministries and within sectors in order to arrive at a (more) common understanding. What was the starting point, what should be the end-state of the work to be undertaken, and how to achieve the goals were questions which needed to be addressed. It is perhaps evident that a common situational picture is the best starting point for all fruitful discussions. However, the difficulties in arriving at such common ground in the cyber domain indicates that such discussions need to take place early, and involve all relevant actors in the different sectors. Finding common ground is also a way of enhancing competence amongst bureaucrats and decision-makers, hence including them in the discussions may prove useful.

Some nations have chosen a more "organisational" approach to the management of competence and strategic lead in the cyber domain by developing new organisational structures for this purpose. The United Kingdom and the Netherlands have established interesting variants of "cyber task force" organisations in government, in order to assist the implementation of policies.[24] Experiences in these nations would deserve further analysis.

Furthermore, the need for broad cooperation between civilian, military, public and private actors in cyberspace was, and will probably remain, a challenge to be handled. The creation of such cooperation in the VDI, as described earlier in this article, is based upon trust and mutual benefit. Trust will take years to build, but it may easily be lost. In a small nation, like Norway, it will be feasible to create an environment of trust and cooperation where the members find that their interests are taken care of. While this may be more difficult in vast nations like the United States, smaller nations may be able to benefit from lessons learned from the VDI in Norway and their decade-long experience in broad cooperation.

On the other hand, foreign investors and companies involved in sub-contracting and the delivery of information and communication equipment to critical infrastructure also operate in Norway. In addition to the challenges caused by globalisation, the system of voluntary

22 Fornyings- og administrasjonsdepartementet et al., Nasjonal strategi for informasjonssikkerhet Handlingsplan (2012), http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Handlingsplan_nasjonal_strategi_informasjonssikkerhet.pdf (accessed January 9th 2013), pages 17-18.

23 One manifestation of differing views can be seen in the responses to the public hearing on the proposed "National Strategy for Cyber Security" of 2010: http://www.regjeringen.no/nb/dep/fd/dok/hoeringer/hoeringsdok/2010/forslag-til-strategi-for-cybersikkerhet/Horingsuttalelser.html?id=599897 (accessed January 9th 2013).

24 See for instance the UK whole-of-government approach of the Office of Cyber Security & Information Assurance (OCSIA), in the Cabinet Office, http://www.cabinetoffice.gov.uk/content/cyber-security (accessed January 9th 2013), and the Task Force Cyber in the Dutch Ministry of Defence.

membership in the VDI may face difficult issues if compared to budgetary restraints. Hence, I believe a broad discussion on alternative ways of ensuring cyber security in Norway, including a regulatory approach, should be expected in the not too distant future.

Further Analyses Needed

Although cyber defence has found a high place on the agenda in many countries, including Norway, there are several issues yet to be solved. For one, discussions on cyber defence should be broadened to also include aspects related to the threat of or the actual use of force, as nations may have to defend themselves in such environment.

One of the major themes to be further discussed is of legal nature. The Norwegian view is that the law of armed conflict also applies to cyberwarfare. This is important as some critics give the impression that cyberspace is a lawless domain. However, there may be several issues related to exactly *how* international law will be applied. What will, in general or in a specific situation, be the threshold for a cyber attack to breach article 2(4) of the United Nations Charter? This article bans the threat or use of force, and it may give a right to self-defence under article 51 of the same Charter, if the use of force amounts to an armed attack. An essential element to consider is that a cyber attack will likely occur in a broader security policy context, which potentially will ease the legal assessment of implications, including determining the aggressor. Several other legal analyses are needed, for example, on how the principle of proportionality will apply to the use of force in cyberspace, how to separate between military objectives and protected civilian information infrastructure (when these are often de facto intertwined), how to handle cyber attacks emanating from a neutral third country (where that country is not in the position to hinder the attacks), or how to manage cyber threats in the build-up of an international security policy crisis – just to mention a few discussion points.

How to coordinate a cyber crisis across government with the appropriate involvement of the relevant actors in the private sector, and while ensuring international information exchange and assistance, would, in my view, also deserve further analyses. We already see the complexities in this domain, both nationally and internationally. It is still hard to imagine the potential impact of a comprehensive cyber attack on the society. Often, discussions on crisis management and preparedness planning in this domain end in a not so fruitful discussion on what is a "realistic scenario" (or not). On the other hand, experiences in crisis management in other domains tell us that one of the essential elements in handling a crisis is to have the relevant structures and procedures in place. As many nations are unwilling to test these structures in large exercises (due to their complexity, but possibly also due to a lack of understanding of the potential implications of a cyber attack), it is difficult to assess the maturity of these structures and procedures in handling a cyber crisis of a certain gravity. Experiences from Estonia[25] and Georgia[26] should be examined and analysed – not only per se, but also as potential lessons identified for other nations. How would my country manage

[25] See for instance "Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security", by Christian Czosseck, Rain Ottis and Anna-Maria Talihärm, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia.
[26] During the war between Georgia and Russia in august 2008, the Georgian government official websites were seriously disrupted, forcing the government to establish alternative websites on Google´s blog-hosting service. The 2008-site can be viewed at http://georgiamfa.blogspot.com/.

such situation? Although the "cyber-Armageddon" or an "Electronic Pearl Harbor"[27] may be more or less realistic, making use of severely challenging scenarios in testing our own structures and procedures would probably not harm our preparation for cyber crises.

Related to this is the diversity of organisations working on cyber issues worldwide, also in the Nordic countries. Apart from cooperation and information sharing between intelligence agencies, the majority of these groups are informal forums for information exchange based on voluntary cooperation between national (official) actors and often including commercial businesses.[28] As long as the main activity of these groups is information exchange in peacetime, this will work well. What happens if there is a security policy situation or an armed conflict? How will these forums work– and will the official forums, such as NATO[29] and others, be sufficient?

Finally, I would like to draw your attention to the need to develop a better system for situational awareness in the event of severe cyber attacks. In traditional crisis management and warfare, establishing situational awareness is a natural part of strategic and operational planning. We have excellent systems for presenting the threat situation, the status of our own and hostile forces, the military strategies and the international cooperation. How would the element of cyber be presented within the existing framework? Do we know what kind of information is critical for the strategic, operational and tactical management of a cyber crisis? Which procedures apply, especially considering the broad civilian (and private) involvement in such crisis – with regard to both threat and consequence management, but also in their potential supporting role to the military? In addition, and not least – how should the government and society at large be able to operate in a situation in which the situational awareness is "impossible", that is, where one cannot trust the systems or the communication infrastructure that we live and work with? I believe also this issue deserves further analyses.

Conclusion

In this article, the aim has been to share a selection of experiences from Norway's quest for enhanced resilience in cyberspace which may be of interest to other smaller nations. In this process, one of the lessons learned was the need to define clearly the roles and responsibilities for cyber defence within the government. This was a major aim of the revised National Strategy for Information Security. Another issue was the shortage of competence on cyber defence within the relevant sectors and the lack of "common ground". Through meetings and discussions within sectors and between departments, as well as with private actors, an increasingly shared situational picture was established. Finally, the Norwegian experience in broad cooperation between civilian, military, public and private actors was described as a potential model for others.

---

[27] See for instance Clarke, Richard A. et al.: Cyber War (2010), as also exemplified in his scenario "Exercise South China Sea", pages 180 onwards.

[28] See for instance Forum of Incident and Security Teams, FIRST (http://www.first.org/) and European Government CERT Group (http://www.egc-group.org/). Among the members in these groups are also the Nordic countries.

[29] The primary coordinating point for operational information exchange in NATO is through NATO Computer Incident Response Capability, NCIRC, http://www.nato.int/cps/en/natolive/topics_78170.htm (accessed January 9th 2013).

I have also pointed to some issues of national and international relevance that I believe deserve further analysis. First, there is unfinished work with regard to how international law applies to cyberwarfare. Second, "worst-case" scenarios should be further explored; not because they represent highly probable scenarios, but because we need to test whether or not our structures and procedures, nationally and internationally, are mature enough to handle a cyber crisis of certain gravity. Finally, further analysis should be undertaken in order to develop a better system for situational awareness during a cyber crisis and the procedures for operating in a degraded information environment.

References

Clarke, Richard A. and Knake, Robert K.: Cyber War. The Next Threat to National Security and What to Do About It, HarperCollins, New York (2010)

Czosseck, Christian et al., Cooperative Cyber Defence Centre of Excellence: Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security, Tallinn, Estonia (2007)

Fornyings- og administrasjonsdepartementet, Justis- og politidepartementet, Forsvarsdepartementet og Samferdselsdepartementet: Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007–2010 (2007)

Fornyings-, administrasjons- og kirkedepartementet, Justis- og beredskapsdepartementet, Samferdselsdepartementet og Forsvarsdepartementet: Nasjonal strategi for informasjonssikkerhet, dated December 17th 2012 (2012)

Fornyings-, administrasjons- og kirkedepartementet, Justis- og beredskapsdepartementet, Samferdselsdepartementet og Forsvarsdepartementet: Nasjonal strategi for informasjonssikkerhet. Handlingsplan, dated December 17th 2012 (2012)

Forsvarsdepartementet, Nærings og handelsdepartementet og Justis- og politidepartementet, Nasjonal strategi for informasjonssikkerhet 2003–2007 (2003)

Forsvarsdepartementet: Støtte og samarbeid. Det moderniserte totalforsvarskonseptet – en oversikt over viktige ordninger og retningslinjer (2007)

Forsvarskommisjonen av 1946 (1946)

Helse- og omsorgsdepartementet: Prop. 1 S 2010–2011 (2010)

Helse- og omsorgskomiteen: Innst. 11 S (2010–2011) om bevilgninger på statsbudsjettet for 2011, kapitler under Helse- og omsorgsdepartementet (rammeområde 15) (2010)

Koordineringsgruppen for IKT risikobildet: Bakgrunnsnotat Cybersikkerhet 2010–06–01 (2010)

Norges offentlige utredninger NOU 2000: 24, Et sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet. Presented July 4th 2000 (2000)

von Rosenbach, Alexander and Keymer, Eleanor, Jane´s Defence Weekly, Issue November 16th 2011: Virtual Warfare (2011)

Cyber Security in Sweden from the Past to the Future

Roland Heickerö

Abstract

Pioneering technologies such as Internet, mobile telephony and computers are driving forces for radical changes of people's opportunities to communicate and spread information. This technological development is basically positive, but there are also detrimental conducts and activities. New threats arise as cyberspace expands. This kind of antagonism cuts through the entire social spectrum and impacts both civilian and military structures, public authorities, organisations and companies, as well as the individual citizen.

In order to handle the threats, all high-technological nations develop doctrines and the capacity to protect and defend functions that are important to society and critical infrastructure. This is also the case for Sweden. From a national perspective, our cyber defence aims at protecting Sweden and Swedish interests against IT attacks from resourceful and advanced players. This includes strategic control and planning, co-operation and co-ordination, as well as operational protection measures.

This text initially provides examples of organisations and activities that presently handle cyber security at national level. After that I describe the development of the Swedish Armed Forces' capacity for cyber defence from the mid-1990s up until the early 2010s. The text ends with a discussion on future information warfare and the challenges that the armed forces face.

Keywords: Sweden, Cyber Security, Civilian authorities, Swedish Armed Forces, Cyber Defence

Cyber Security at the National Level

There are both similarities and differences in the structure and concentration of the state administrations in the Nordic countries. In Sweden, the activities of the authorities are directed through instructions and regulations from the Cabinet Office via the departments. In accordance with Swedish administrative law, the authorities have a relatively independent role. Since the country does not have a ministry of the interior in the broad sense, no ministry is solely responsible for the issue of cyber security; the responsibility is divided between several ministries – defence, justice, and industry and commerce.

Subordinated to these, there are a number of authorities that handle issues surrounding information security. The most important of these include the Swedish Civil Contingencies Agency (MSB), the National Defence Radio Establishment (FRA), the Swedish Post and Telecom Agency (PTS), the National Police Board (RPS), the Swedish Security Service (SÄPO), the Defence Materiel Administration (FMV), and the Swedish Armed Forces.

The Swedish Civil Contingencies Agency

The task of the Swedish Civil Contingencies Agency, MSB, is to support and co-ordinate the work on public information security, and to analyse and assess the development in the world in this field.[1] The agency provides advice on and support for preventive work to other state authorities, municipalities and county councils, as well as to companies and organisations. Examples of support include information on how to implement and apply control systems for information security, based on international standards in the ISO 27000 series.

The Swedish Civil Contingencies Agency reports to the Government on conditions in the field of information security and supports society by preventing and handling IT incidents. In co-operation with other authorities, the Swedish Civil Contingencies Agency has produced an information security strategy for society on behalf of the Government. This strategy remains in force during the period 2010–2015, and it designates a direction with long-term goals for society's information security. The strategy is supplemented by a national action plan with concrete proposals for measures. The strategy is updated, in collaboration with other authorities, at least every six years.

When the Swedish Civil Contingencies Agency was formed on the 1st of January 2009, it assumed responsibility for the *SAMFI* co-operation group. SAMFI consists of a number of authorities with special tasks in the field of information security. The group meets six times per year; the purpose is to facilitate the co-operation through exchange of information and co-ordination. Apart from the Swedish Civil Contingencies Agency, the authorities that form part of SAMFI include the Swedish Armed Forces, the Defence Materiel Administration, the National Defence Radio Establishment, the Swedish Post and Telecom Agency, the National Police Board/Swedish Security Service.

As a supplement to SAMFI, the Swedish Civil Contingencies Agency in September 2009 also established a national information security council for co-ordination of the public administration and Swedish industry, consisting of a number of participants who represent large parts of the information infrastructure that is important to society.

CERT-SE

CERT-SE is Sweden's national Computer Emergency Response Team, tasked to support society in handling and preventing IT incidents. As of the 1st of January 2011 CERT-SE is with the Swedish Civil Contingencies Agency, before that it was subordinated to the Swedish Post and Telecom Agency. Its tasks include acting quickly in connection with IT incidents, co-operating with authorities with special tasks in the field of information security and representing Sweden in contacts with the corresponding agencies in other countries.

[1] https://www.msb.se/

The Defence Materiel Administration and CSEC

The Defence Materiel Administration purchases equipment for the Swedish Armed Forces and authorities in the civilian security sector. It is a civilian, independent authority subordinated to the Ministry of Defence. Information security is an important part when purchasing and implementing defence equipment systems, services and processes.

CSEC is an independent body within the Defence Materiel Administration; it is Sweden's national certification body for IT security in products and systems.[2] It was set up in 2002 after a government decision. It performs impartial reviews of products' IT security, in accordance with the international ISO/IEC IS 15408 standard, also known as Common Criteria, including products used by the Swedish Armed Forces.

CSEC issues internationally approved certificates for companies that examine IT products. It performs oversight of these companies and supports them in their review work. Internationally CSEC co-operates with other certification agencies and security services.

The National Defence Radio Establishment

The National Defence Radio Establishment (FRA) can be described as one of the foundations of the national cyber defence. It is an independent civilian authority with two main tasks: national information security and signals intelligence.[3] The National Defence Radio Establishment's instructions include maintaining high technical skills in the field of information security and supporting state authorities and state-owned companies that handle information that it assessed to be sensitive from a vulnerability point of view or in a security and/or defence policy context.

The National Defence Radio Establishment above all has to be able to:
- support efforts during national crises with IT features;
- assist in identifying the players involved in connection with IT-related threats against systems that are important to society;
- perform IT security analyses, penetration tests and IT forensics;
- provide other technical support.

The National Defence Radio Establishment is also responsible for providing civilian authorities and companies that are important to society with SIGINT-proof equipment that has been approved by the Swedish Armed Forces, equipment that makes electronic exchange of classified information possible. They also develop cryptographic solutions and participate, together with other authorities, in national and international IT security exercises, such as *Cyberstorm*[4] and *NISÖ 2012*.

One proposal from the institute has been to establish a national technical warning and detection system (TWD) in order to discover and counteract IT attacks directed against

[2] http://fmv.se/csec
[3] http://www.fra.se/
[4] http://www.dhs.gov/cyber-storm-securing-cyber-space

activities that are important to Swedish society and critical infrastructure.[5] The purpose of such a detection system is to sound the alarm for attempted, on-going, and successful penetrations. This includes locating specific components that have been infected and cleaning up the infection, but also carrying out a forensic analysis and an assessment of the damage caused by the event. A TWD consists of sensors, a communications solution and a central function for analysis. The sensors analyse traffic in the network with the aid of signature and deviation analyses. When an IT attack is discovered, a warning is sent both to the subject of the attack and the analysis centre.

The TWD can be seen both as a tool for information security and as a part of an intelligence function. It is mainly passive. However, the system can become more active through increased functionality; automatically take the appropriate protection measures from generated alarms, block traffic, both in cases of penetration from the outside and illicit extraction of information from the inside.

Other Civilian Authorities

Other authorities that handle information security include the Post and Telecom Agency, which monitors electronic communication and the postal service in Sweden, the National Police Board and the Security Service. The National Police Board among other things contains the IT crimes squad with resources for IT forensics. In the Swedish Security Service there are units that handle issues surrounding national security in cyberspace.

The Swedish Armed Forces

The Swedish Armed Forces closely monitor the development of threats in cyberspace and develop capacities, doctrines and strategies for protection and defence of vital information infrastructure and critical information. Cyber security is a prioritised activity and an integrated part of the Swedish Armed Forces' tasks; in its instructions it is specified as protection against armed attacks, upholding territorial integrity, etcetera.

All branches and units contain implemented IT security functions. The responsibility for cyber defence primarily lies with the Military Intelligence and Security Service (MUST) and the Swedish Armed Forces' Network and Telecommunications Unit (FMTM). The electronic warfare battalion and the psyops company also work in the information arena.

The Development from the 1990s

Information warfare as a phenomenon began to be discussed within the Swedish Armed Forces in 1994–1995.[6] An official letter on the need for an elucidation of the responsibility was handed over from the Defence and Traffic committees to the Government in 1995,

[5] Formulation of a technical detection and warning system for activities and infrastructure that are important to society. Account of the Government's assignment to the National Defence Radio Establishment. Registration number: 03200:3419/10:11.
[6] Interview with Lars Nicander, head of the Centre for Asymmetrical Threats (CATS) at the National Defence College, 29 October 2012.

which in 1996 led the government defence bill work group to order two reports on the subject from the Ministry of Defence starting in 1997.[7] One was the *ASTA study*, an assignment from the government that included a number of authorities, principally with military links.

The other was the work group for protection against information warfare, *WG IW,* which functioned as an internal report to the Cabinet Office. The Ministry of Defence chaired, the secretariat was located at the Swedish National Defence College. There was participation by authorities from several sectors of society, not just military ones, including the Ministry of Industry and Commerce, the Security Service, the National Police Board/the National Bureau of Investigation (RKP), the National Board of Psychological Defence (SPF), the Defence Research Agency (FOI), the National Defence College, and the Armed Forces (MUST and the Military Unit Command, KRI). However, the National Defence Radio Establishment and the Defence Materiel Administration, which were part of the ASTA study, were not included in WG IW.

The assignment included specifying the state's responsibility, showing how work on security can be fit into the national action programme for IT and how the work with IT security issues should be organised and divided between different state authorities. One result of WG IW when it comes to policies was that information warfare should be seen as an operational issue, just as in the U.S. and Germany at this time, and not as an intelligence issue. Examples of proposals that were presented in the WG IW study included setting up a comprehensive crisis management organisation for IT security at national level and a "State CERT". Another proposal was to gather the responsibility for co-ordination of the work on IT security in the public administration at one place. The ASTA study was completed on the 1st of July 1997 while WG IW's main report was issued in 1998 and formed part of several government bills.[8]

As a result, a national CERT (CERT-SE) was established, initially within the Post and Telecom Agency, but it was subsequently transferred to the Civil Contingencies Agency in 2011. The studies also laid the foundation for the idea of setting up a specific IT defence unit (Red Team unit) with CERT functions for the Armed Forces.

For various reasons, the issue of where IW should be housed passed from operations to intelligence. In the 2000s there were a number of inquiries on both this and responsibility for information security. In 2012 it passed from intelligence back to operations. One reason for this was changes in the rest of the world when it comes to the view on offensive and defensive cyber warfare, and to the development of new threats on Internet. In 2012 the Ministry of Defence initiated a study with the ambition of producing information for a national cyber strategy. The National Defence College is responsible for this.

[7] Excerpt from the Ministry of Defence's "control station bill" of March 1999. (Bill 98/99:74.)
[8] Bill 98/99:74.

The Present Cyber Defence

The Armed Forces Headquarters and the Military Intelligence and Security Service

In the Armed Forces Headquarters central command, the head of the Military Intelligence and Security Service (MUST) is responsible for the security protection service, which among other things includes information security and SIGINT protection.[9] The Technical Office of the Military Intelligence and Security Service has established a section for IT security development. The purpose is early implementation of the right IT security architecture and security mechanisms so that information and critical systems are given sufficient protection. Before being put into operation, the section participates in the work on reviewing and providing an expert opinion in order to make sure that security is satisfactory.

MUST is also responsible for the field of cryptography and supports the Cabinet Office in matters related to this subject in international work groups in the EU.

The Swedish Armed Forces' Network and Telecommunications Unit (FMTM)

The Swedish Armed Forces' Network and Telecommunications Unit, FMTM, is a constantly updated rapid deployment unit that works both nationally and internationally, on the whole preparedness scale.[10] The unit is responsible for the Swedish Armed Forces' technical telecommunications infrastructure; it has activities in several locations in the country. FMTM includes the IT defence unit (ITF).

The IT Defence Unit (ITF)

The IT defence unit was set up in 2004. Its task is to protect the Swedish Armed Forces' infrastructure for information and command systems against attacks and maintain a high level of IT security in the authority. This is done both through preventive security, penetration detection and monitoring of other nations and players. Neutralising attacks also requires an understanding of various kinds of attack methods. As opposed to MUST, ITF is an operational rapid deployment unit, with everything that means.

The unit's employees are carefully selected and characterised by a high level of technical skills. Training and capacity building are given a lot of scope since the field of IT security is both knowledge-intensive and in constant change.

Within ITF there is a function designated *FM CERT* (Computer Emergency Response Team) which handles IT security incidents in the Swedish Armed Forces. It also analyses and suggests improvements of its activities from an information security perspective.

[9] http://www.forsvarsmakten.se/hkv/Must/
[10] http://www.forsvarsmakten.se/fmtm/

FM CERT

FM CERT is a resource at military strategic level when it comes to IT security. The organisation has two main tasks, *incident management* and *situation reports*.

Incident management involves collection and compilation of IT security-related incidents. In less serious incidents FM CERT normally has only an advisory and supporting function, compiling statistics and informing on experiences. In more serious incidents FM CERT can step in and coordinate and/or take charge of the incident management. The other main task involves compiling and distributing situation reports when it comes to the IT security situation in the Swedish Armed Forces' IT systems. Ultimately, it aims at providing the head of operations good information for decisions.

The situation reports are primarily based on monitoring of the rest of the world and incident reports. The monitoring of the rest of the world also serves to inform operators of vulnerabilities and available security updates.

Other Units in the Information Arena

Other units that work in the information domain include the 13th electronic warfare battalion and the 10th psyops unit, both located at the Command Regiment.[11]

The electronic warfare battalion is a unit with advanced technical telephony and computer systems that are used to detect, survey and position opponents, gather intelligence, and jam and deceive communications, the latter through false signals. The battalion is involved in international efforts for instance in Afghanistan during the Swedish engagement in the country.

The task of the psyops unit is to influence specific target groups in a number of ways. This is done physically, e.g. through leaflets, and over the airwaves. They support all kinds of units in an operations area with tactical psyops efforts. The unit also appears autonomously and can perform independent information collection.

The Future

In a future perspective, information warfare is an integrated part of every major military and political conflict, and cyberspace is both its own dimension and a co-ordinated part of the other physical arenas, such as Land, Sea, Air and Space. Information warfare takes place all over the whole spectrum of the combat zone, at all levels: strategic, operational and tactical with different main emphases during different phases. A conflict can be both started and decided in the digital sphere, without kinetic means having to be used. Means for information warfare, both offensive and defensive, can be used individually or in combination with other weapons systems.[12]

[11] http://www.forsvarsmakten.se/ledr/

[12] Heickerö, R. (2012) *The Dark Side of the Internet. On Information Warfare and Cyber Threats*. Peter Lang GmbH. Internationaler Verlag der Wissenschaften. Frankfurt am Main, Germany.

In a military context, information warfare is either seen as a reinforcement, a force multiplier, to military operations or as an individual and vital capacity in itself.

The development of the Armed Forces' future capacity is to a large extent ruled by the threats and the technical development in ICT.[13] At the technical level there is a convergence between the computer and the telecom worlds, between wire and wireless communications, which can be exemplified by smart phones. A far-reaching "IP-fication" facilitates the development towards an "all connected network" where access to and spreading of information takes place in many different ways and in many kinds of media and networks.[14]

The convergence is a driving force for the development of a joint capability for information warfare for all of the Armed Forces, where computer and network operations are merged with electronic warfare and psychological operations. An integrated communications environment with demands for immediate access to information creates opportunities for influence.

During an information operation where a specific target is going to be approached, the appropriate method is selected from the toolbox, irrespective of whether it is electronic warfare, IT warfare or psyops, related to the situation, location, requirements and the desired effect. The need for increased co-ordination puts demands on existing military structures and handling of resources, just as development of joint methods, processes and nomenclature. Additional driving forces for a stronger integration of capacities are the continuous demands for cost rationalisations and an efficient use of resources, which will probably increase in the future.[15]

A possible future scenario is to establish a national information warfare capacity for all of the Armed Forces that includes all the components for defensive and offensive measures in the electromagnetic spectrum and cyberspace. Co-ordination can be physical at a central unit and/or logical. If necessary, key resources can be distributed to all arenas depending on the situation and location, for example, during international efforts. Another scenario is that each arena has its own information warfare capacity which is co-ordinated and led at central level. The technology makes both these scenarios possible. Such a development will demand new methods and processes.

Other fields that are being developed include automated collection, sensor information and analysis of events. There is a concentration on creating robust information infrastructures and effective security handling both technically and administratively. Co-operation and exchange of information is becoming increasingly important. At authorities, routines are being set up for incident reports and information sharing between the different CERTs, to other authorities, to the private industry and to international organisations. Co-ordination, exercises and exchange of information with skilled and well-informed parties internationally is a priority for the Armed Forces as well as for other authorities that are in charge of national cyber security.

[13] ICT – Information and Communication Technologies.
[14] Heickerö, R., Lindahl, D., Sommestad, T., Gustafsson, T., Gudmundson-Hunstad, A. (2012) Technical Forecast. Cyber security in a 2035 perspective. FOI-R--3472—SE. Stockholm, Sweden (in Swedish).
[15] Heickerö, R. (2010) Information Warfare 2030. FOI-R--3040—SE. Stockholm, Sweden (in Swedish).

A Rugged Nation

Simo Huopio

Abstract

In this article the Finnish Security Strategy for Society dated in late 2010 is analyzed from the perspective of cyber threats in 2012. Conclusions are clear: cyber threats cannot be treated only as an isolated phenomenon. Instead, they need to be analysed in conjunction with other major threats in which the cyber domain plays a significant role as an enabler. A point is raised which goes beyond critical infrastructure protection: in order to counter cyber threats resiliently information systems have to be specified, procured, produced and used in such a way that everybody participating in the process shares a common vision on what is to be protected, in which way, and feels proud of being part of the process.

We have to strive for more usable and bug-free systems in supporting our nation. In other words, we have to become a rugged nation. The key themes of the article are taken from the Rugged Software Initiative and extrapolated from software application development to critical infrastructure protection in a small independent state. In this approach security strategies could be tied to practical action without gaping chasms. A rugged nation could even make its citizens proud of the national IT instead of forcing them follow when large IT system projects fail one after another.

Keywords: Finnish Security Strategy, Cyber Threat, Rugged Software Initiative, Nation

The Finnish Security Strategy for Society 2010 and Cyber Threat

The Finnish Security Strategy for Society [YTS2010] was published at the end of 2010. The strategy was a replacement for the Government Resolution on Securing the Functions Vital to Society from 2006 [YETT2006]. The strategy is defined as the common basis for preparedness and crisis management for all actors in society. Special emphasis is stated to be on the harmonization of the preparedness activities of the ministries, on addressing better the international dimension, and on the improved enumeration of the actors.

After having stated the objective, the respective actors are listed with their generic responsibilities. The strategy discusses preparedness by listing 13 identified threat scenarios (Table 1). These scenarios constitute an approach that is emblematic of the whole strategy. The strategy paper was the first one to name cyber threats as a distinct vertical threat scenario. The same concepts were discussed in 2006, but only as a part of more generic "disturbances in electrical infrastructure".

The cyber threat scenario is revised from the previous strategy paper and it addresses the threat landscape more broadly. Even after the update, the scenario is too superficial and it does not offer a coherent description of the challenges. The fundamental problem is that

the scenario isolates cyber threat and the overall cyber element from the other major threat scenarios. This has had the result that the collateral effects which contribute to the other threat scenarios are left mainly without notice. In addition, the strategy paper assumes that systems and software supporting the CIP are not by themselves significantly contributing to the overall threat to the infrastructure by being buggy or brittle by design.

Serious disturbances in the power supply
Serious disturbances in the telecommunications and information systems - cyber threats
Serious disturbances in transport logistics
Serious disruptions in public utilities
Serious disturbances in food supply
Serious disturbances in the financial and payment systems
Disturbances in the availability of public funding
Serious disturbances in the health and welfare of the population
Major accidents, extreme natural phenomena and environmental threats
Terrorism and other criminality that endanger social order
Serious disturbance in border security
A political, economic and military pressure
The use of military force

Table 1: A list of Threat Scenarios in YTS2010

Currently, there is no separate cyber threat. In terms of critical infrastructure, cyber disruptions are unlikely to happen without major effects on other vital functions than just the pure communication systems and/or the public Internet-based services. Therefore, cyber threats should be viewed as a horizontal threat element relating to practically all threat scenarios.

After having listed the threat scenarios, the strategy continues by going through the top level vital functions (Table 2). For each of the functions, the desired end state is uttered and it is backed up by assigning specific strategic tasks for every relevant ministry.

Management of Government affairs
International Activities
Finland's defense capability
Internal Security
Functioning of the economy and infrastructure
The population's income security and capability to function
Psychological resilience to crisis

Table 2: A list of vital functions in YTS2010

By looking into the content of these chapters in the strategy, one can notice that there are several references to the criticality of certain ICT systems, both in the end state and in the strategic tasks. In these references, the links between the multitude of ICT systems and the critical vital functions are described much better than in the separate chapter describing the cyber threat scenario.

In one of the appendices of the strategy, almost as an afterthought, there is a detailed table of specific disturbances which is cross-correlated with the threat scenarios in a large matrix. This presentation takes the pervasiveness of cyber threat into account quite well.

2012 Perspective to Cyber Threat

There are few significant changes in the year 2012 perspective to cyber threat when compared to the times of the 2010 security strategy.

Internet-facing software is under an intensive scrutiny. A very large number of individuals or research groups with different backgrounds are trying to find security vulnerabilities from browsers, media viewers, web service platforms, web applications, and so on. This is both a good and a bad thing. The quality and robustness of applications are evidently getting better. A bigger proportion of consumers and companies using the software is also applying the related security patches timely – partially, thanks to being helped by automatic update mechanisms. The bad thing is that it is evident that there are numerous bugs in the software that are not published or even found yet. Without keeping up with the updates, for a reason or another, one really becomes publicly vulnerable.

The security updates are not necessary installed at the time of their publication in systems where they could disrupt the normal operation by downtime (which is unwanted in, for example, manufacturing facilities) or by incompatibility with other applications if applied without extra testing (for example, in various company intranets). If Internet connectivity is needed for administrative or other purposes, specific firewall and Intrusion Detection/Prevention (IDS/IPS) systems are set up to filter out malicious traffic that might use the known vulnerabilities to penetrate the systems. If a computer system is logically or physically separated from Internet, the risk of intrusion is traditionally considered to be much lower. Therefore, the security updates, which have to be brought in manually, are applied at a lot slower pace – if at all.

Recent studies have shown that having firewalls with reactive defenses tuned up is not enough. The flexibility of the TCP protocol gives almost infinite possibilities to format and split the traffic into packets of practically arbitrary size and frequency. By playing with these parameters the attacker can find a combination with which he or she can disguise malicious traffic to pass through the perimeter defenses. While there is hope for building better firewalls, there is a lot of work for the industry to do. [CERTFI2011] [STONE2010]

Advanced big budget attacks, which can be conducted by using zero day vulnerabilities and spreading mechanisms via USB sticks or other media, have proven that even the air gap is not enough, if there is enough interest to reach the protected target. The existence of Stuxnet, Dugu or Flame – and malware similar to these – is an undeniable proof that having an unpatched or badly administered system is always a risk, even without any network connectivity. [WIRED2011]

A commonly used approach in the protection of individual computers has been to make sure that security updates are applied promptly and that the Anti-Virus scanning software – often including a personal firewall – is up-to-date. Today, even the spokespersons of prominent Anti-Virus companies confess that their products do not protect the customer from the most advanced attackers. [FSC2012b]

The brittleness of the interconnected, ever growing ICT systems has become even more evident than before. Many major IT projects have ended up with some sort of public failure. Usually, the security aspects do not play a part in these failures, because even the basic functionality of the systems fails due to bad planning, bad procurement and/or sheer complexity of the systems. [Kivek2012]

The picture of the adversaries has also been clarified. While the nation-state level adversaries with increasing resources are more openly planning for the ability to penetrate the protected systems, the inherit brittleness of the systems leaves plenty of room for hactivists to demonstrate what can be achieved with an excuse, enough free time, and a guest for good laughs [Olson2012]. On the background, criminal groups do their own intensive research on how to game and how to exploit all possible money related aspects.

Security updates, diligent administration, firewalls and AV are still very necessary, for the long tail of the history of computer attacks is available for everyone to feast upon. The question is how to keep the systems secure when all traditional methods of securing them are failing? The answer is: we have to demand, define, procure, and make them inherently more secure. At the same time, we have to make sure that we can recover better from successful attacks by crafting real and proven recovery plans and backup systems. We just have to be more secure, more rugged to withstand it all.

Starting Points for Making Things Work

The Rugged Software Initiative

The Rugged Software initiative is a fresh approach to software security coined by a small group of software engineers. The initiative is centered on being proud of and responsible for the code that one has created; and while being this, also making the code rugged to withstand everything the world will throw at it. A pair of quotes from the introduction of the Rugged Handbook [Rugged2012]:

> *"Rugged" describes software development organizations which have a culture of rapidly evolving their ability to create available, survivable, defensible, secure and resilient software.*
>
> *Rugged is NOT the same as "secure." Secure is possible state of affairs at a certain point of time. But rugged secures staying ahead of the threat over time.*

While the rugged manifestos and whitepapers concentrate mainly on the software company culture, which is very important in order to produce a rugged code, they also give many simple but useful ideas about how to adapt to the strategic level things outside the world of software R&D.

One of the aforementioned ideas is to make security visible with a specific and understandable "security story" which captures everything necessary to understand why the code and the organization that built it are Rugged. The ingenious thought behind this is to construct the

security stories in plain English and thus, readable and understandable to all. Therefore, everyone can comment on and commit to them – and together turn them into a selling point, a requirement definition and a working document. Another central takeaway is the co-existence and co-operation of "breakers" and "builders" who continuously strive together to make the product rugged.

Another prevalent approach to being rugged is pride and positivity. Taking pride in the security posture of the whole company and of the code it produces quite naturally affects one's approach to the quality of the end results. Positivity is brought forth also in many ways: the security stories describe the security posture in a positive and productive way, the security requirements are stated in a positive light instead of being deemed as endless threats, innuendo and restrictions. The inevitably higher cost of the product is justified by underlining what a rugged, great quality the product entails – instead of troubles. While the Rugged Software may have some work to do to really convert the industry and to scale the Rugged approach from application development to bigger systems, I still try to pick the low-hanging fruits of the approach for a security strategy level use in the next chapter.

The Liability of Software Vendors

Another starting point for improved software in the critical infrastructure is to take a different approach to software procurement. Much can be done by just tightening requirements and being a much more knowledgeable buyer. However, with this approach one can end up paying a disproportionate share of the vendor's security work – a cost (and risk) which should be spread evenly between all clients and also the other companies that the software vendor relies on. A natural option for allocating the software risk more evenly would be the introduction of a liability of software vendors. [Cont2012]

Introducing this kind of liability could really make software products more secure. It has been argued that a company is more likely to take precautions and really to strive for achieving due diligence in software security, if putting their product on the market forces the company to assume liability for it. In addition to enhancing product quality, the company would, most probably, like to spread the risk to the other vendors who have supplied modules or libraries that are used as a part of the end product. If the injured/harmed party was compensated for real damages (subject to the legislative/normative guidance), this would, most probably, introduce some kind of new insurance instruments to spread the costly risk further. [Cont2012] All of these approaches are already in use in the world of product safety – maybe it would be a good time for a big push to introduce them also to software products.

Continuing with Compliancy Approach – and Making the Most of It

A lot of work has been done at the national levels in producing a wide set of guidelines, compliancy tools, and auditing tools for security. In Finland, the most usable result from this work is the National Security Auditing Criteria (KATAKRI, [Defmin2011]). KATAKRI is a normative criterion for organizations and systems that handle classified information, and a good reference for any company. Work on the criterion continues in order to give more

practical and coherent information to help meeting the criterion, and also to audit against it. The Government Information Security Management Board (VAHTI, [VM2012]) has produced a set of guidelines to give good all-round advice for keeping the IT systems safe.

On the international arena, the standard bodies have been active. To pick a new effort which is worth following: the emerging ISO/IEC 27034 standard on Application Security has the first part already published and the rest of the standard is in progress [ISO2011]. There are also some commercial initiatives to help companies in the introspection of their approach to software security, of which a good example is the Building Security in Maturity Model (BSIMM) [Cig2012]. SAFECode whitepaper on Secure Software Development, again, is a vendor-independent starting point with a great selection of design principles, coding practices and verification guidance [SAFE2011].

The challenge with the compliancy route is that the used standards and criteria are usually of so high level that, actually, they do not help producing better, more secure software with fewer bugs. In worst case, bad implementation of this approach generates a lot of extra work and bureaucracy; it has only negligible effects on the actual software; and it gives a very bad name to all things labeled as "security". Possible mandatory reactive measures and security testing do have their effects, but the actual software creation is affected only indirectly.

The Compliancy Approach has actual potential to make software more secure, if a good national or a global standard on software security management can accomplish changes in the actual development work. A broad adoption of such standard in the requirements work and the usage of liability as leverage are essential to this slow progress.

A Rugged Nation

How a small nation with limited resources could become a Rugged Nation, which keeps its critical infrastructure secured from cyber threats?

As we are well aware of what our vital functions are, we should create security stories for the security posture of each of them. The key change to the past is to write the story in a manner that everybody can read, understand, and commit to. While following the rugged principles the same security story should be told on all levels; the level details and confidentiality could be adjusted according to a layered approach. For example, one layer could introduce the technical principles for designing and fortifying a particular system, while another layer could tell the average citizens how the state and the electricity grid companies together make sure that the grid controls are rugged and simpler to maintain in exceptional circumstances. [Rugged2012]

Politicians must keep in mind that the security story idea is not only a good catch to be used once during the electoral contest, but a true commitment paper which evolves throughout the life cycle of the critical system. It ties hands and resources to sustainable work for a long period of time – yet, for a reason. The content of the story could include, for instance,

- What is protected and against which threats?
- What are we prepared to do when the planned protection fails?
- What are we prepared to do when the whole system X is M.I.A.?
- What are the key data points for multiple levels of trust?
- What is the liability breakdown from the user to the vendor of the system X and to the regulator?
- How to uphold the commitment to update the story; to keep it up-to-date for its whole lifecycle?

At which level of details the story should exist? There is plenty of room for experimentation, but here are a few examples

- *Public on-line services are trustworthy, resilient and available to everybody despite the situation.*
  - this could be enhanced with clear incentives for the third party Internet services to be Rugged

- *Data collected of private individuals for the use of public services is kept available for everybody the individual agrees it to be delivered.*
  - how data is kept safe and separate from that collected of others; and how it can be reviewed and deleted at will of the owner should be explained

- *Utility management (electricity, water, sewage, heat) control data is kept on a separate rugged network with fail-safes and backup communications.*
  - The security story would continue with a description of the first and secondary level fail-safes, the order in which the possible disruptions are managed, and the available options for individuals to prepare emergency power generation for their households.

In more practical terms, the whole process of turning to a rugged nation should follow the same principles as the equivalent process in a large corporation: The top level commitment to being rugged should be clearly stated and held. The security of the critical systems should be a matter of national pride which every citizen should be committed to keep in a good shape. The national strategies should be tied to concrete activities without changing the language in between. Cyber threat should be treated as horizontal threat to the basic enablers instead of keeping it as a separate threat scenario.

The systems procurement should follow the principle of aiming for simplification and usability in all systems. The systems are long-term investments which include the support arrangements throughout the expected lifespan. In addition to the software vendor committing to due diligence in maintenance, the vendor could be kept liable for system failures in most critical functionality of the product. The liability is spread throughout the support network and it also covers the state customer who should be able to find out whether the system is vulnerable to each newly published security bug. In addition to recognizing the bugs, the customer should actually be able to make the necessary fixes by him- or herself in an urgent situation.

The global safety, security and robustness standards should be followed and their use should be mandated in normative legislation and procurement processes. Vendors and individuals own initiatives would be rewarded; if a superior security posture is acquired in a new and innovative way, it should result in better scores in procurement competition or better compensation to the people who actually made it happen.

Security research should be nurtured in a country by a culture of innovation in the universities and research facilities. Security competence should be built within the state employers, in the local industry supporting the CI, and in a healthy academic/research community with common long-term targets and pride.

Pride should be the driving force that keeps healthy competition alive between the builders and the breakers. This competition would also establish a fruitful balance within the state. Knowledge gathered in this process should also be utilized in all aspects of national cyber defense. If there is a mandatory or voluntary military service, it should be used as a platform to educate the citizens to follow the best security practices and to gather suitably talented individuals to a voluntary cyber defense league.

Conclusion

The Security Strategy for Society 2010 is a solid construction, but it lacks intuition to treat cyber threat as a horizontal phenomenon that affects almost all aspects of the critical infrastructure. The recent changes in the cyber threat picture enhance the need to address the horizontality even further – traditional security measures are failing to keep up with the adversaries. Only way to survive with pride is to take a new approach and to become rugged to the bone.

References

[CERTFI2011] CERT-FI Vuosikatsaus 2011, http://www.cert.fi/katsaukset/2011/vuosikatsaus2011.html

[CERTFI2012a] CERT-FI Tietoturvakatsaus 1/2012 http://www.cert.fi/katsaukset/2012/tietoturvakatsaus_1_2012.html

[CERTFI2012b] CERT-FI Tietoturvakatsaus 2/2012 http://www.cert.fi/katsaukset/2012/tietoturvakatsaus_1_2012.html

[Cig2012] The Building Security In Maturity Model - BSIMM4, September 2012, downloaded from http://bsimm.com/download/ web version available at http:://bsimm.com/online/

[Cont2012] "Software and product liability", Giuseppe Contissa / European University Institute, 13.04.2012 http://www.slideshare.net/aliasnetwork/software-liability

[FSC2012] F-Secure Threat Report H1 2012-09-19 search/Threat_Report_H1_2012.pdf

[FSC2012b] Blog entry by Mikko Hyppönen: On Stuxnet, Dugu and Flame, 2.6.2012, http://www.f-secure.com/weblog/archives/00002376.html

[ISO2011] Website: ISO Standard description, ISO/IEC 27034 Information technology — Security techniques — Application security http://www.iso27001security.com/html/27034.html http://webstore.iec.ch/webstore/webstore.nsf/mysearchajax?Openform&key=27034

[Rugged2012] Rugged Handbook (strawman) v7, Rugged Software, August 2012, https://www.ruggedsoftware.org/wp-content/uploads/2012/09/Rugged-Handbook-v7.docx

[STONE2010] Press release: "Newly Discovered Threats Pose Serious Risk for Organizations Worldwide" http://www.stonesoft.com/us/press_and_media/releases/us_english/2010/18102010.html

[Defmin2011] Ministry of Defence, National Security Auditing Criteria (KATAKRI), version 2, 2011 http://www.defmin.fi/files/1871/KATAKRI_eng_version.pdf

[MoF2012] Ministry of Finance, The Government Information Security Management Board introduction, http://www.vm.fi/vm/en/16_ict/03_information_security/index.jsp

[Kivek2012] Blog entry by Otso Kivekäs, 24.9.2012
http://otsokivekas.fi/2012/09/it-hankintaprojekti-sairastaa/

[Olson2012] We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency, Little, Brown and Company (June 5, 2012), ISBN 978-0316213547

[SAFE2011] Fundamental Practices for Secure Software Development, 2nd Edition - A guide to the Most Effective Secure Development Practices in Use Today, SAFECode, 8.2.2011, www.safecode.org/publications/SAFECode_Dev_Pracitces0211.pdf

[YTS2010] Security Strategy for Society, Finnish Goverment Resolution 2010, http://www.defmin.fi/files/1883/PDF.SecurityStrategy.pdf http://www.yhteiskunnanturvallisuus.fi/en/materials

[YETT2006] The Government Resolution on The Strategy for Securing the Functions Vital to Society 23.11.2006 http://www.defmin.fi/files/858/06_12_12_YETTS__in_english.pdf

[WIRED2011] "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History",
Wired "Threat Level" blog post by Kim Zetter, 07.11.2011,
http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1

Contaminated Rather than Classified: CIS Design Principles to Support Cyber Incident Response Collaboration

Erka Koivunen

Abstract

Many attacks in the cyber domain seek to exploit weaknesses in Communications and Information Systems. In doing so, they pose a threat to the very technical foundations of our networked data processing and information society at large. The art of containment, extraction and analysis of malicious computer code artefacts can be likened to working with hazardous materials. All it takes is one unsuspecting click of a mouse and the security of one's CIS is breached. Analysts seeking to analyse and share such artefacts need to operate in specialised computing environments that expose as little attack surface as possible while still providing enough means to observe the behaviour of the malicious payload. Creating and maintaining such an environment is not an easy task. Adding to the complexity is the need to incorporate the highly networked and collaborative working methods of Computer Security Incident Response Teams. CSIRTs have mastered the art of information sharing and collaborative incident response between geographically dispersed and temporally asynchronous teams. Up until now, however, information has been shared at unclassified level only. The Nordic countries have now taken the bold move to create a network for inter-CSIRT collaboration at classified level. This paper outlines the design principles adopted by CERT Finland for its internal operating environment "IRTI" and draws parallels to the Nordic CERT Information Sharing Network.

Keywords: Information security, network security, CERT, CERT-FI, CIS, CSIRT, NCIS, information sharing, artefact handling, security breach, network attack, abuse, computer break-in, malware.

Introduction

Network and security incidents are situations where effects harmful to security have manifested or have had potential to manifest in the networks or in the networked information systems. The need to handle ever-increasing number of incidents has forced many organisations to establish specialised teams dedicated to incident response. [16, 17] These teams are often called Computer Security Incident Response Teams (CSIRT), or CERTs, but other terms such as abuse helpdesks, security teams — and lately, Cyber Security Centres — have also been used. [5, 3]

An unavoidable aspect of working with CSIRT is the routine exposure to malware and other malicious payload. In the context of this paper, malicious payload refers to data content in the form of software code or network traffic that seeks to disrupt the normal operations of the Communications and Information Systems (CIS) by exploiting vulnerabilities and

configuration weaknesses in any of the systems that participate in the transmission, storage and handling of the payload in terms of parsing or executing. Malicious payload is the very poison that the attackers use to break in and to gain unauthorised control over the system, or to exhaust its resources to cause denial of service conditions. If successful, the attacks violate the confidentiality, integrity and availability which are characteristics of the system.

While one would normally want to keep the malicious payload deactivated and out of their operational CIS, the CSIRTs explicitly want to collect and analyse as much artefacts of malicious nature as possible to assist in their analytical work and to support incident response. Due to the complex nature of CIS, new software vulnerabilities will always be found, erroneous systems configurations will be put into production, and people using CIS will keep making poor security judgements.

Examples of instances in which CIS have been particularly vulnerable to malicious payload include a) a collection of vulnerabilities in SNMP implementations found by OUSPG in 2002 [20, 4], b) Windows Metafile vulnerability in late 2005 and early 2006 [19, 18], c) a collection of cross-platform TCP denial of service conditions found by Outpost24 in 2008 [7], and d) a wealth of network evasion techniques extensively researched by Stonesoft since 2010 [8, 9]. Common to all of these examples is that even fully patched and reasonably hardened systems were defenceless if put in touch with the malicious payload. Clearly, CSIRTs need to pay a considerable amount of attention in setting up their own CIS infrastructure as the payload put through them may turn out to be hazardous.

In this paper, the high-level design principles of two specialised CSIRT environments are described: CERT Finland's internal network, codenamed IRTI, and the Nordic CERT Information Sharing Network, abbreviated NCIS [21, 23].

CERT Finland

CERT Finland (CERT-FI) is the national Computer Security Incident Response Team of Finland, a unit of Finnish Communications Regulatory Authority that operates under the Ministry of Transport and Communications. CERT-FI is the so-called CSIRT-of-last-resort [12, 6] for the Finnish networks. While its services are available to entire Finland, the primary constituency consists of operators of critical infrastructure and telecommunications providers.

Typical incidents that CERT-FI handles include denial of service attacks, malware, system break-ins and software vulnerabilities. Most incidents take place in public communications networks or in systems connected to public networks.

The majority of incident data handled by CERT-FI can be characterised as "sensitive but unclassified" or fall under the lowest security classification levels, thus allowing some degrees of freedom in terms of security clearance procedures and in the design of the supporting CIS.

IRTI

The operational environment that CERT-FI uses for bulk of its tasks is called IRTI. The Finnish word *irti* stands for *detached, at large*, *loose,* or *adrift*.

The primary definition of the name appropriately describes one of the principal features of the system: the aim is to keep material handled by CERT-FI separate from the rest of the agency's CIS infrastructure in a way that helps contain possible security breaches from crossing from one security domain to another. Additionally, the more subtle nuances of the word *irti* suggest that the system used by CERT Finland enjoys added degrees of freedom from the national information security standards [14] point of view and that the system has been custom-built to support the extraordinary nature of tasks performed by CERT-FI staff. [22]

In order to support CERT-FI's mission, a set of design principles and implementation choices for IRTI were laid out.

Summary of IRTI Design Principles

No secrets IRTI environment is not designed with the protection of classified material in mind. While conforming to most aspects of KATAKRI [14], IRTI adds caveats in areas such as liberal access to public networks, deliberate introduction of malware into the system, and omission of anti-virus products in parts of the system. For the routine incidents handled by CERT-FI, information about exploit methods, attack vectors and malware samples are not considered particularly sensitive. Almost invariably, the technical details of the threat have been obtained from public networks and have already been made publicly available. Conversely, the contextual incident information such as the identity of the plaintiffs, attribution to the perpetrators, knowledge about the attack's impact and evaluation of the effectiveness of the protective controls is sensitive and in many cases, classified. Even in cases where the incident as a whole would be classified, a wealth of technical details and artefacts can still be analysed in unclassified environment once extracted and separated from the general substance and context.

Minimal attack surface While not promising to protect secrets, IRTI aspires to be resistant against active payload and immune to exploits. CERT-FI staffers routinely investigate networks in the murky parts of Internet and examine known and suspected samples of malware. In order to protect the user and the system from inadvertent infection and other security breaches, the tools in IRTI cannot be susceptible to the type of threats described in Chapter 1 of this article. Particularly important is that, unless specifically ordered, the tools in IRTI must not parse and process the payload. For instance, file system permissions in IRTI must be modified in a way to prevent execution of active content and privilege escalation; automated indexing of file system contents must be turned off; anti-virus products must be inactivated; document preview functionality must be disabled; and web browsers must be replaced with tools, such as *wget,* which do not try to rampantly parse and execute the payload before its true nature can be determined.

Separated and contained IRTI has been built with the worst-case scenario in mind. IRTI is a collection of systems and segmented networks with varying degrees of connections between each other. If a security breach occurred in one corner of IRTI, it should neither be allowed to spread into the whole CIS, nor to break out from one container to another. Conversely, IRTI should not be affected by a security breach in surrounding networks. Special sandboxes systems are introduced where suspected copies of malicious software can be executed in controlled environment.

Autonomy Essential IRTI services should continue to function and remain accessible even under network failures or limited availability of other computing resources. Additionally, IRTI employs its own configuration and user management.

Small is beautiful As the system has been built gradually and over the course of many years, it has become a mosaic of small independent components. Lately, some additional attention has been paid to ensuring the smooth interplay of individual components. Abuse Helper [1] has been found to be of immense help for it provides a means to pass data and commands between individual components. It can be said that CERT-FI runs its own botnet. [11]

Terminated access Not all IRTI services are accessible on a network level. In situations in which end users cannot be trusted to connect into the back office network directly or initiate outbound connections, access is limited to application level through terminal services and remote shells.

Authenticated and Logged Users and systems connecting to IRTI are put through a strong authentication mechanism. IRTI logs user, system and network level actions, and employs CERT-FI's own HAVARO [10] system for network security anomaly detection.

Mobile Selected tools and data in IRTI are accessible regardless of where the work is done. The user simply needs to connect to the network, authenticate oneself and start using his or her applications.

Client-agnostic Most tools and data in IRTI can be accessed from devices running a variety of operating systems. That does not mean, however, that any client system can be plugged into IRTI regardless of its configuration. As the devices are effectively the endpoints in encrypted network communication, they must be hardened and operated in secure fashion.

Cheap IRTI has been built mostly in-house by using commercially available or free components. CERT-FI has rather limited spending power in CIS items, which makes open source products nearly a necessity. IRTI is constantly evolving as new features are implemented and out-dated portions are scrapped. The CERT-FI staff members know the system inside out as they have contributed to its development in a very personal fashion. However, there is also a downside to the in-house development: support contracts with external specialists cover only portions of the network, that is, "if you break it, you fix it."

Connected to Internet Selected systems in IRTI must be able to communicate with Internet. After all, that is where most security incidents take place and where they are countered. CERT-FI staff members are frequent travellers and may need to access the systems while on

the road. The duty officers are on-call round the clock for emergency response, and they expect that the systems are accessible non-stop from wherever they happen to be when the call comes in.

Further Work

Traditional classified networks are generally badly suited for rapid and voluminous information exchange and for collaborative working methods employed by the CSIRTs. According to CERT-FI's experience, a dramatic decline in work productivity takes place when incident handling is conducted through classified channels.

This is particularly frustrating in incidents in which the technical incident indicators are unclassified or even public knowledge, but for some reason cannot be easily removed from the rest of the protectively marked substance.

A frequently occurring incident type involves specially crafted portable document format files (pdf) which seek to infect the victim's computer upon opening the document. [13] At least in theory, the technical incident indicators and the attack code should be easy to extract from the document contents.

Since systems from different security domains cannot be trusted enough to be directly interconnected on a system level, special emphasis should be put to the development of tools that support the extraction of the technical exploit portions of the file while discarding the classified portions of the content.

Nordic Cooperation on Cyber Security

In 2008, the Foreign Ministers of Denmark, Norway, Iceland, Sweden and Finland commissioned the former Foreign Minister of Norway, Mr. Thorvald Stoltenberg to draw up a list of proposals for a closer foreign and security policy cooperation between the Nordic countries. The report, published in early 2009, presented thirteen proposals grouped in seven categories. One of the proposals was titled "Nordic resource network to protect against cyber attacks", and it called for support to the creation and cooperation of Nordic national CSIRTs by creating secure communications network to connect the teams and to foster collaboration. [23] In 2010, the Nordic Foreign Ministers agreed to establish a secure communications network for the Nordic CERTs as a first step in Nordic Cooperation on Cyber Security. [21] The network should be running by the end of year 2012.

Nordic CERT Information Sharing Network

The Nordic resource network, according Mr Stoltenberg's report, consists of the national computer security incident response teams of Nordic countries: Danish GovCERT, NorCERT from Norway, CERT-IS of Iceland, CERT-SE from Sweden and CERT Finland. At the time of writing this article, the Nordic countries have signed the General Security

Agreement [15] and the first phase of the secure communications network, the Nordic CERT Information Sharing Network (NCIS), is nearing its completion.

The primary goal of NCIS was to create a highly secure collaborative working environment that supports national CSIRTs in their information exchange and collective analytical work in incident response. With the introduction of NCIS, the Nordic CSIRTs now have the technical means to exchange classified material, which is a necessary addition to the existing modes of cooperation.

The classified nature of NCIS appears to be in contrast to IRTI. Before deciding, whether the two systems complement or contradict each other, let us present some of the guiding principles behind NCIS.

Summary of NCIS Design Principles

Classified NCIS is a system approved for transmission and storage of classified information between the participating CSIRTs. Operating in classified environment brings about added administrative burden that is most markedly manifested in the mandatory separation of NCIS from other CIS, especially Internet. The separation does not only serve to protect the system from network-based attacks, but it also enforces the "no read-up" and "no write-down" rules as described in the Bell-LaPadula security model [2].

Malicious content What makes NCIS distinct from other classified systems is the fact that it is specifically built to accommodate the exchange, analysis and storage of artefacts of malicious kind as described in Chapter 1. As a precautionary measure, only operational staff members from the national CSIRTs will be approved to access NCIS.

Collaborative and pro-sharing In the course of time, a range of tools to assist in information sharing and online collaboration in incident response will be introduced in the NCIS network. Examples of these kinds of tools are wikis, malware repositories and instant messaging. Examples of the shared information include classified editions of IDS signatures and other indicator information, assistance in artefact analysis, malware samples, incident reports, and tools. Many of the candidate tools have already been used in public networks but will now be re-introduced in classified environment, thus allowing for deepened cooperation.

Distributed Services in NCIS can be introduced in a distributed fashion, thus allowing participating teams to contribute to the infrastructure by adding internally developed services to the NCIS network and by allowing other teams access them. This fosters innovation and recognises the fact that the CSIRTs oftentimes need to build the tools of their own, because ready-made solutions do not exist. NCIS can be considered a trusted platform where participating teams can share access to otherwise unavailable tools.

Cheap NCIS will only be used by a limited number of organisations and a conservative number of users, which helps simplify the network design and keep operations and

maintenance overhead to a minimum. For most of the participating teams, the low cost of the system is crucial.

Further Work

NCIS is not yet fully operational and it will be further developed in the coming years. It is evident that, if successful, networks similar to NCIS will be established elsewhere in Europe. However, it cannot be stressed enough that while the network components and configuration can be replicated with moderate ease, no information sharing can take place until the General Security Agreements have been mutually ratified by the participating countries and a reasonable level of trust has been accumulated among the participating CSIRT organisations and their representatives. Furthermore, it must be noted that NCIS is a specialised environment designed by CSIRTs to CSIRTs and it may not meet the needs of other kinds of users and missions.

Conclusion

CERT-FI's IRTI operating environment is a collection of networks and tools that support the handling of unclassified incidents. IRTI simplifies the development, adoption and maintenance of the hardened CIS that CERT-FI employs to contain, extract and analyse artefacts of malicious software and attack traffic in a unified fashion. IRTI is designed in a way that makes it resistant to attacks and helps contain problems, if a security breach occurs. Components of IRTI are allowed connect to Internet and seek to exploit the venues for unclassified collaboration between CSIRTs, Abuse Helpdesks and operations centres all over the world. IRTI is not suitable for routine handling and exchange of classified material. The Nordic CERT Information Sharing network, NCIS, is a novel attempt to recreate some of the collaborative tools in a classified environment shared by the national CSIRTs of the five Nordic countries – Denmark, Norway, Iceland, Sweden and Finland. NCIS enables the participating teams to exchange classified information and to access each other's tools and services in a secure and controlled fashion. NCIS complements the existing unclassified systems by providing a secure platform for the Nordic countries to join forces in combating common cyber threats.

IRTI is the bread and butter of any self-respecting CSIRT. NCIS is the missing (communications) link that helps bring the appointed national CSIRTs together to resolve difficult cyber security incidents of classified nature. When combined, the systems will undoubtedly bring CERT Finland's incident response capabilities to a new, higher level.

References

1. AbuseHelper source code [referenced 20121114], https://bitbucket.org/clarifiednetworks/abusehelper/wiki/Home

2. Bell, D. E., Secure Computer Systems: A Refinement of the Mathematical Model, Mitre Corporation (1974) [referenced 20121114], http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=AD0780528

3. CERT Coordination Center, Authorized Users of "CERT" [referenced 20121113], http://www.cert.org/csirts/cert_authorized.html

4. CERT Coordination Center, CERT® Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP) (2002) [referenced 20121113], http://www.cert.org/advisories/CA-2002-03.html

5. CERT Coordination Center, CSIRT FAQ [referenced 20121113], http://www.cert.org/csirts/csirt_faq.html

6. CERT Coordination Center, CSIRTs with National Responsibility [referenced 20121113], http://www.cert.org/csirts/national/

7. CERT-FI, Advisory on the Outpost24 TCP issues (2009) [referenced 20121113], https://www.cert.fi/haavoittuvuudet/2008/tcp-vulnerabilities.html

8. CERT-FI, Advisory on IDS/IPS device vulnerabilities that may circumvent protections (2010) [referenced 20121113], https://www.cert.fi/en/reports/2010/vulnerability385726.html

9. CERT-FI, Advisory on further IDS/IPS device vulnerabilities that may circumvent protections (2011) [referenced 20121113], https://www.cert.fi/en/reports/2011/vulnerability487536.html

10. CERT-FI (ed.), Proceedings of the 6th Annual CIP Seminar [referenced 20121114], http://www.cert.fi/esitykset/2012/cip-seminaari2012.html

11. Eronen, J., AbuseHelper: Fighting botnets with botnets, presentation at T2'12 infosec conference in Helsinki, Finland

12. European Network and Information Security Agency, ENISA: Baseline capabilities for national / governmental CERTs (Part 1 Operational Aspects), version 1.0 (initial draft), ENISA (2009) [referenced 20121113], http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities

13. F-Secure weblog, DHS PDF (2008) [referenced 20121113], http://www.f-secure.com/weblog/archives/00001449.html

14. Finnish national security authority, National Security Auditing Criteria (KATAKRI) version II, (2011) [referenced 20121113], http://www.defmin.fi/National_Security_Auditing_Criteria

15. General Security Agreement of the Mutual Protection and Exchange of Classified Information between Denmark, Finland, Iceland, Norway and Sweden [referenced 20121114], http://www.finlex.fi/fi/sopimukset/sopsviite/2010/20100128

16. Koivunen, E., Effective Information Sharing for Incident Response Coordination: Reporting Network and Information Security Incidents and Requesting Assistance (2010) [referenced 201211-13], http://iki.fi/Erka.Koivunen/Studies/DI/DI_Erka_Koivunen.pdf

17. Koivunen, E., "Why Wasn't I Notified?": Information Security Incident Reporting Demystified, NordSec'10 Proceedings of the 15th Nordic conference on Information Security Technology for Applications, pp. 55-70, Springer-Verlag 2012

18. Microsoft Security Bulletin MS06-001 – Critical, Vulnerability in Graphics Rendering Engine Could Allow Remote Code Execution (912919), Microsoft Security TechCenter 2006 [referenced 20121113], http://technet.microsoft.com/en-us/security/bulletin/ms06-001

19. National Vulnerability Database, Vulnerability Summary for CVE-2005-4560 [referenced 20121113], http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-4560

20. Oulu University, PROTOS Test-Suite: c06-snmpv1 (2002) [referenced 20121113], https://www.ee.oulu.fi/research/ouspg/PROTOS_Test-Suite_c06-snmpv1

21. Rasmussen, K., N., Erklæring fra nordisk utenriksministermøte – Reykjavik, 3. november 2010, [referenced 20121113], http://www.regjeringen.no/upload/UD/Vedlegg/Nordisk%20samarbeid/erkl_reykjavik2010.pdf

22. Selén, K. CERT-FI IRTI-ympäristön kuvaus, Finnish Communications Regulatory Authority (2012), [document protectively marked]

23. Stoltenberg, T. Nordic cooperation on foreign and security policy, Proposals presented to the extraordinary meeting of Nordic foreign ministers in Oslo on 9 February 2009 [referenced 20121113], http://www.regjeringen.no/upload/UD/Vedlegg/nordicreport.pdf

Part III:

Cyberwar

Cyberwar: Another Revolution in Military Affairs?

Tero Palokangas

Abstract

The article challenges the latest thoughts about cyberwar as a kind of revolution in military affairs or as a domain of war by itself. The best way to survive in current and future cyberwars is to develop own C4-systems in a determined way, so that one can be certain and confident about all of the processes and applications in use. Information assurance and security must be tightly connected with cyberwarfare. Without vulnerabilities there are no cyber threats – excluding the human nature and behaviour, which remain to be the most important threats in future cyberwarfare.

Keywords: C4-system, Cyberwar, Computer Network Operations, Information assurance, Information security, Revolution in Military Affairs, Vulnerability

About Cyberwarfare

Warfare has been divided into five dimensions; a three-dimensional space, time, and the electromagnetic spectrum. Lately, cyberspace has been argued to be the 6th dimension of modern warfare. Cyberspace management has become an important part of modern warfare.[1] The appearance of cyber threats has still not completely removed the threat of traditional use of military force; only the range of means has expanded. It is likely that in future crises cyber means are used increasingly to affect both military and civilian targets in co-ordination with traditional means of war fighting.[2]

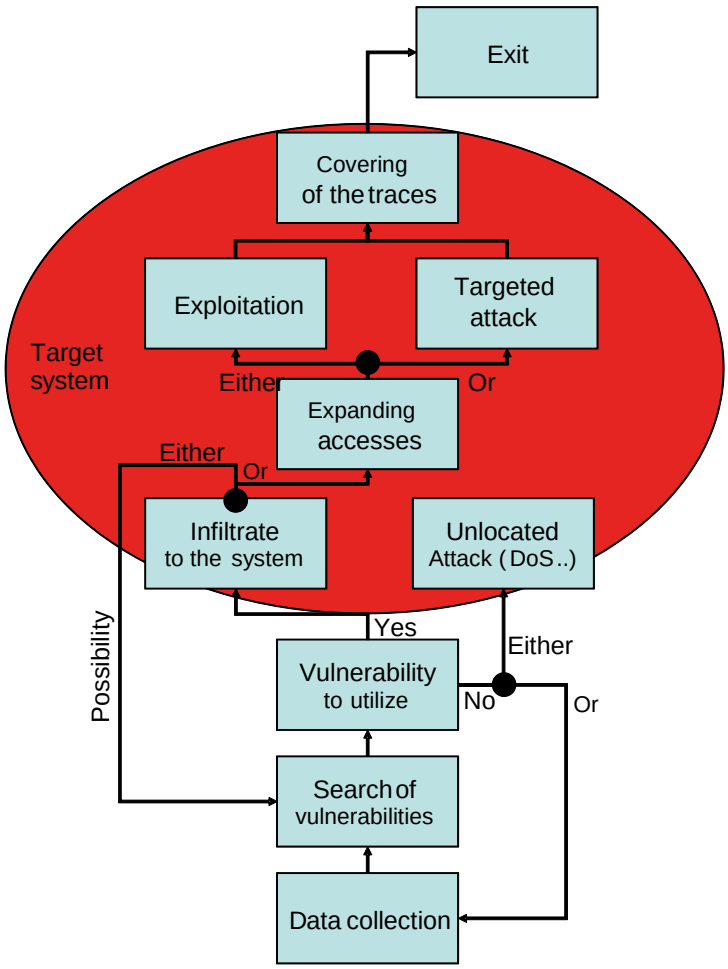
Influencing computer network differs significantly from traditional kinetic means of influence. It is typical of cyber attacks that the caused indirect effects are usually more important than the direct effects. The effects are generally very difficult to estimate. Particularly, targeted intelligent cyber attacks are often complicated. Their design and implementation requires a significant amount of human knowledge and capital. To build a cyber weapon is usually relatively inexpensive, even if the developed methods are often disposable. The major factor with regard to cyber weapons is that their origin is reasonably easy to hide (anonymity). Cyber weapons are versatile methods because they can be used in almost every possible security situation.[3]

Information operations planning, and Computer Network Operation (CNO) as part of it, should be carried out as an integral part of the overall operational planning process. The aim

[1] Kosola, Jyri: *Development of Technology and its effects to warfare 2015–2025*, Department of Military Technology, National Defense University, Helsinki, 2010, page 2–3.
[2] Puheloinen, Ari: *Speech of CO FDF at Helsinki 8.11.2010*, http://www.puolustusvoimat.fi/wcm/su+puolustusvoimat.fi/puolustusvoimat.fi/puolustusvoimat/perustietoa/puolustusvoimain+komentaja/puheet/puheet+2010, 10.1.2011.
[3] Owens, William A., Dam, Kenneth W. ja Lin, Herbert S. (edited): *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, National Research Council, Washington, 2009, page 19–20.

in every situation is to support the overall mission objectives as much as possible with all available performance. Computer network operations should be planned at the highest level to make sure that all activities are connected tightly with strategic communication and the key messages we are trying to deliver.[4]

The conflict between Georgia and Russia proved that authorization to use force in cyber operations should be delegated to the tactical level. This ensures the best possible ability to protect one's own networks, and to be able to quickly influence the vulnerabilities of the opponent's dynamic networks. It is likely that in time-critical situations the best way to succeed in cyber operations is to authorize the CNO units to conduct the needed operations. Some of the targets of cyber operations are very sensitive. There is always the risk of unwanted effects on our own or on a third-party information networks and systems. In some cases, it may be necessary to set up some constrains dealing with the use of cyber force. One option is to regulate cyber operations by pre-defined rules of engagement.[5]



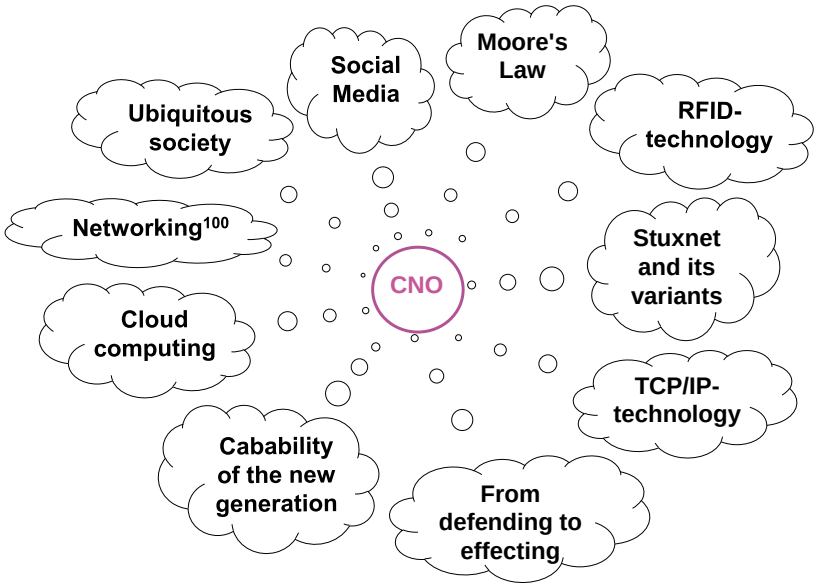
Picture 1: Computer Network Operations' kill-chain[6]

[4] Allen, Patrick D.: Information Operations Planning, Artech House, Norwood, 2007.
[5] Rios, Billy K.: Sun Tzu was a Hacker: An Examination of the Tactics and Operations from a Real World Cyber Attack, *The Virtual Battlefield: Perspectives on Cyber Warfare*, Czosseck, Christian ja Geers, Kenneth (edited), IOS Press BV, Amsterdam, 2009, page 145–154.
[6] Carr, Jeffrey: *Inside Cyber Warfare*, O'Reilly Media, Sebastopol, 2010, page 152–157.

Computer Network Operations in 2030

Possible megatrends of the future's information society are:
- Increased need for real-time information
- Increased transparency
- Convergence of media platforms- New generation's capability to operate in cyberspace
- Increased possibility to navigate in different medias
- Increased necessity to share information
- Emphasis on swarm intelligence
- Emergence of ubiquitous society
- Increase in the complexity of the work tasks
- Increase in the value of work value- Systems development according to the iterative model
- Emphasized enterprise architecture management and development[7]

From the computer network operations' point of view, societies are becoming increasingly dependent on information technology. This trend will accelerate in the future, when the responsibility for the development of our networks will be given to the generation that has actively worked and lived with computers all their lives. Cloud services will become more common, that is, the most important information resources will be online in the future. Knowledge sharing will be emphasized even further, and it will provide a significant scope for social engineering. The significance of social media will increase, and it might become the main form of communication. Blogs will spread even more malware than they do now. People will find it difficult to use social media in a transparent way and at the same time make sure that an appropriate level of information security and assurance is exercised.[8]



Picture 2: Some megatrends affecting future cyber operations[9]

[7] Inkinen, Sam: Speech at FDF Social Media seminar, Helsinki, 8.12.2010.
[8] Interview of Majewski, Klaus & Kiviharju, Mikko & Tauriainen, Aki & Candolin, Catharina, autumn 2010.
[9] Illi, Mikko & Karppinen, Mika & Palokangas, Tero & Seppälä, Pasi: Computer Network Operations in the Year of 2030, *Strategic Communication and Information Operations 2030*, Sirén, Torsti (edited), Department of Leadership and Military Pedagogy, National Defense University, Helsinki, 2011, page 175.

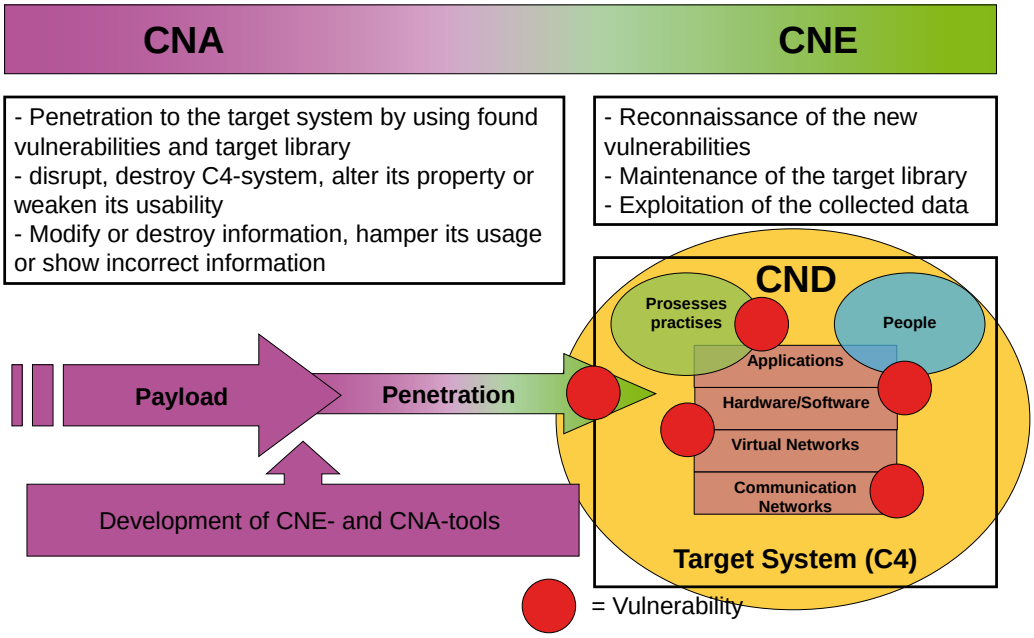
In the future, everything will be controllable. Situational awareness will be even more difficult to achieve because of the huge amount of information. Processing all available information is going to be a challenge. Radio-frequency remote identification (RFID) technologies will be spread all over and thus, offering more opportunities for cyber operations. The rise of TCP/IP-technology in the military C4-systems will mean more vulnerability to worry about. It will also mean a significant amount of work to develop robust and secure applications for the future "battlefield". The amount of transmitted data grows explosively, which makes cyber defence even more challenging. On the future's networked battlefield, the focus will likely be on the development of attacking/affecting systems, since in almost any case one will be a step behind, if one is concentrating on passive defending systems only.[10]

Cyberwarfare, C4-systems, Information Security and Information assurance

C4-systems are all the time becoming more difficult and complex to understand and handle. Even our own laptops are sometimes way too labyrinthine to monitor and to make sure that all processes are working in a proper and intended way. Therefore, it is no wonder that large stranded C4-systems are as vulnerable as they seem to be on the basis of some recent incidents in cyberworld. Behind the scenes of the late attacks and crimes, targeted to the adversary's C4-systems, has usually been some kind of unwise and careless human behaviour. People are not aware what their computers, routers and switches are performing at certain moments. The rise of cloud computing, social media and the outsourcing of our basic functionalities are clear and present dangers of which the security authorities must take care in the future. Simultaneously, the authorities must cut down their expenses, which is not making the task easier – vice versa. All of the rising threats in cyberworld will need to be handled with contracting budgets.

Information security and information assurance are basic counteraction elements, when we are talking about vulnerabilities in and threats to our C4-systems. We must make sure that we know well enough all software and hardware in use. It is no secret that back doors and other implementations in hardware coming from certain parts of Asia have been found. We must have the instruments and the procedures to make sure that the equipment we are using is clean from a possible adversary's intelligence and affecting tools. Software is even more tricky business because the numbers of applications are voluminous, and most of them are in a desperate need of constant updates – otherwise they will not work effectively. There must be tight rules about who, when, where and how is entitled to update our software.

[10] Majewski & Kiviharju 2010.



Picture 3: Dependence between C4-systems, vulnerabilities and cyber methods (CNA = Computer Network Attack, CNE = Computer Network Exploitation, CND = Computer Network Defence).

What make defending in the cyber domain even more difficult are the different interconnected applications and their behaviour. The so-called blended attacks are cyber attacks conducted by using two or more vulnerabilities in different applications. An individual application's security is usually designed against the most likely threats. As a rule, other software and applications are not taken into account in programming. Software is generally operated independently, and the exchanges of information with other applications are handled with mere assumptions. Contemporary information systems are manufactured by many different vendors, and the possible security risks between the different applications are normally taken very poorly into account. It is possible to find out what kind of information sharing the different subsystems will generate with each other when influencing a part of the whole system. This gives an opportunity to achieve the desired effects on the target system by influencing some other system that is connected to the real target system. The performance of individual programs and applications evolve and become more complex, which gives more and more opportunities for blended attacks in the future.[11]

In the future, the capabilities of each system element are primarily a part of the entire information system, and only secondarily particular capabilities. That is why the need for coordination in the development of systems is growing rapidly.[12] Coordination between different cooperating programs and projects is vital. The difficulty of predicting the future means that all systems must be modular and component-based. This will inevitably lead to the fragmentation of large integrated systems that consist of smaller independent, but interconnected systems. This requires the architectural solutions to be service-oriented, and the use of open solutions. The whole architecture of the systems shall be controlled at the

[11] Dhanjani, Nitesh, Rios, Billy and Hardin, Brett: *Hacking: The next generation*, O'Reilly Media, Sebastobol, 2009, page 91, 102–103, 118–120.
[12] Kosola 2010, page 54–56.

system level, as well as at the level of single subsystems. System requirements should be made by focusing primarily on environmental conditions. In addition, the boundaries should be clearly determined. This is to ensure the system modularity and compatibility, as well as to create the conditions for continuous development and long-term management of the life cycle.[13]

Conclusion

In some occasions, cyberwar has been claimed to be yet another revolution in military affairs. It has also been argued that cyber could be a war fighting domain by itself. I am not saying that cyber should not been a domain by itself; it well could be. However, this depends on how we see our future and how we define the big picture of military affairs and domains – possibilities for that are almost unlimited. The best way of surviving cyberwarfare is to develop our own C4-systems in a proper and determined way, so that we are certain and confident about all processes and applications we are using. Information assurance and security must be connected tightly with cyberwar and the cyber domain. Without vulnerabilities there are no cyber threats. That is, of course, a utopia, since there will always be vulnerabilities to be taken care of. Nevertheless, each vulnerability we are able to eliminate by the means of information security and comprehensive development of our C4-systems, is a single win in the continuous battle between good and bad in cyberspace.

The human nature and behaviour are essential parts of cyber security. No matter how good we are at the technical development of our C4-systems, there will always be people using those equipment and applications. Social engineering has been one of the most successful cyber methods. People and their goodwill are so easy to take advantage of. In some occasions, infiltration to the target system most likely needs the kill-chain to use social engineering. That is why we have to educate and train our people to handle different kinds of situations in which one might get fooled. Acting securely on C4-systems needs, in addition to decent social skills, basic knowledge of information technology and its applications. If one does not know at all where his or her computer and networks are connected to and how his or her activity on those forums might be dangerous, one is definitely not in a good position on the cyber battlefield. At the end, the most important threats in cyberwarfare are the human nature and behaviour.

The Nordic countries have a lot in common in the cyber domain. We are all very dependent on networks. Our societies will not last very long, if our vital networks go down. Our countries are also too little players in the cyber domain to get along alone with some big players. That is why there is a lot to be won in cyber defence, if we really cooperate with each other. The Nordic countries share an interest in planning, developing and using common cyber capabilities. Examples of cooperation amongst the Nordic countries could be:

– compound computing capabilities for cyber defence purposes
– secure number of interconnections in global networks
– unified national CERT-organizations and know-how
– synthesized developing and acquiring of cyber defence tools, techniques and procedures

[13] Kosola 2010, page 57–59.

– promotion of shared cyber defence objectives at the international theatre
– agreed on support to any Nordic country in the cyber domain when needed

Picture 4: Network worms are one of the basic threats in cyberwarfare

One could say that an independent country may have some caveats in the use of her sensitive cyber tools. My opinion is that the Nordic countries should not have any major caveats or secrets with regard to cyber weapons. At the end, there is nothing new under the sun; not even in cyberworld. Cooperation can give us so much more than we are ever able to achieve alone. Cyber matters could be also a clear and necessary area of cooperation, for example, under the umbrella of NORDEFCO. Cyberwarfare is not future, it is today. That is why we must be ready and cooperate. Otherwise, we are preparing ourselves for the past and, at the same time, for an incorrect war or conflict.

What comes to the Revolution in Military Affairs, I think that the rise of cyberwarfare is not a revolution. To me it is more like a common evolution of the military affairs, because things have developed, and will always develop, to be more effective and versatile. Socialization has become more and more dependent on information technology and interconnected systems. That is why cyber threats must be taken very seriously. Cyber defence and Computer Network Operations must be an integral part of the nations' and armies' organizations and capabilities. To me cyber is not by itself a war fighting domain, even though I consider it as a critical part of modern warfare: cyber consists of different dimensions of physical, psychical and information domains. The best way of surviving cyberwar is to make sure that we are totally confident about the security of our own C4-systems. On top of that, we must have a sufficient toolbox of active capabilities. Otherwise, we are the sitting ducks of cyberwarfare.

References

Allen, Patrick D.: Information Operations Planning, Artech House, Norwood, 2007.

Carr, Jeffrey: Inside Cyber Warfare, O'Reilly Media, Sebastopol, 2010.

Czosseck, Christian ja Geers, Kenneth (edited): The Virtual Battlefield: Perspectives on Cyber Warfare, IOS Press BV, Amsterdam, 2009.

Dhanjani, Nitesh, Rios, Billy and Hardin, Brett: *Hacking: The next generation*, O'Reilly Media, Sebastobol, 2009.

Inkinen, Sam: Speech at FDF Social Media seminar, Helsinki, 8.12.2010.

Kosola, Jyri: Development of Technology and its effects to warfare 2015–2025, Department of Military Technology, National Defence University, Helsinki, 2010.4

Majewski, Klaus & Kiviharju, Mikko & Tauriainen, Aki & Candolin, Catharina, interviews, autumn 2010.

Owens, William A., Dam, Kenneth W. ja Lin, Herbert S. (edited): Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, National Research Council, Washington, 2009.

Puheloinen, Ari: Speech of CO FDF in Helsinki 8.11.2010.

Sirén, Torsti (edited): Strategic Communication and Information Operations 2030, Department of Leadership and Military Pedagogy, National Defence University, Helsinki, 2011.

What Can We Say About Cyberwar Based on Cybernetics?

Sakari Ahvenainen

Abstract

"What Can We Say About Cyberwar Based on Cybernetics?" article examines the basics of cyberwar, mostly cybernetics. It also deals with cyberspace as a new global infrastructure and cyberwar as a global level of warfare. The focus of the article is also on the types and levels of cybernetic information and their importance in cyberwar. It also studies the human and the computer as cybernetic systems and as targets of cyberwar. Ahvenainen points out eight logical types of cyberwar and claims that essentially Sun Tzu's and Clausewitz's understandings of warfare similar to the cybernetic process and that John Boyd's OODA loop is a cybernetic process. According to him, computer programs and integrated chips combined with human understanding comprise the heart of cyberwar.

Keywords: cybernetics, cyberwar, sensor, decision making unit, effector, computer, programs, data, information, interpretation of information, global, internet

Motto 1: The new paradigm of warfare in the global era is strategic communication.[1]

Motto 2: The worldwide internet is the new stage of warfare in the global era.[2]

Introduction

Motto 1 and 2 have been chosen by the author as the focal point of this article which examines cyberwar from the viewpoint of cybernetics. The foundation for the article is cybernetics, the etymological context of cyber. Cybernetics is the science of the control and communication of animals and machines. In the article, the term "cyberwar" is used to mean organized hostile cyberspace-assisted influence during either peacetime or wartime. "Cyberspace" is the structure created by physical computers, physical communications and other infrastructure for digital information. Its most important, although not sole component is Internet.

The method used in this article is evolutionary induction, first introduced by Austrian-British professor and philosopher of science Karl Popper. It condenses the process into an interesting problem and tentative theories (theory), as well as sorts out mistakes and creates new problems.[3] The objective of the article is to answer the following question: what can be said about cyberwar based on cybernetics, the basic theory of systems dealing with information?

---

[1] Lieutenant Colonel and Doctor of Political Science Torsti Siren (2011), p.12-3. However, there is not a single mention of "cyber" or any of its derivatives in the book.
[2] US Secretary of Defense Leon Panetta as in Kotilainen (2012). More specifically, "The internet is the new stage for warfare."
[3] Popper (1979).

Cybernetics and Systems Theory

In this article cybernetics is examined through Popper's theory of evolutionary induction. In the article Popper's method is used, but the theory will not be explicitly written out due to the length of the article. The viewpoints of cybernetics will be evaluated in regard to cyberwar. Next warfare as a cybernetic system will be assessed. Finally, assessments will be made along with eliminating mistakes, followed by the article's conclusions: on the basis of this article, what can be said about cyberwar on the basis of cybernetics? Some of the conclusions lead to new problems, which is a natural part of the process.

Cyberwar originates from the tremendous growth of efficiency and volume in computer technology. Development has given rise to, for instance, precision guided weapons. An important early example of the impact of computers and electronics are the battles of the Bekaa Valley in 1982, approximately 30 years ago. Within ten minutes Israel destroyed 17 out of 19 anti-aircraft missile units and later shot down 85 Syrian aircraft without losses. The result was affected by the integrated cooperation of all units, using computer-related components such as electronic reconnaissance and jamming, frequency-hopping radios, airborne early warning aircrafts (E-2C Hawkeye), the artillery and aircraft's precision guided weapons[4] (air-to-ground), radar-seeking missiles, air-to-air missiles and reconnaissance and decoy drones.[5] This example illustrates that the technologically weaker side may be dangerously vulnerable to the technologically superior side. This is nothing new apart from the extent and global nature of the phenomenon: a computer is present in nearly all technical systems and the technology in question is global.

Cybernetics is a part of general systems theory.[6] Cybernetics was originally the science of *control and communication* of animals: "Cybernetics: or Control and Communication in the Animal and the Machine."[7] Cyber originates from the Greek language and means the navigator of a ship or the art of navigating, moving towards a preset objective. Cybernetics is the study of systems that consist of subsystems and, in particular, the study of *the relationship within the system and its parts* in time. When the organization in time is purposeful this is called control.[8]

The basic components of cybernetics, the system that operates with information, are: (1) a receptor (sensor) for the acquisition of information/data about the environment and the system itself, (2) the coding of the observations by the decision making unit into commands, (3) an effector for influencing the surrounding environment or the system itself, as well as (4) feedback for the control of the functioning of the different parts of the system to reach the objective.[9]

In cybernetics, *information is always connected to an existent physical system, that is, information is always physical.*[10] As a result, the communicated information only has relevance in relation

[4] "Precision guided weapon" in the context of this article is a weapon with a cybernetic system: a receptor (sensor), a decision making unit, and an effector.
[5] Clary (1988).
[6] Skyttner (2005) & Bertalanffy (2003), p.17, 21, 22.
[7] Wiener (2000).
[8] Turchin (1977), p. 17.
[9] Turchin (1977), p.25 & Skyttner (2005), p.91 & Paloheimo (2002), p. 111.
[10] Turchin (1977), p.17 & Gleick (2011), p.355-372.

to the system, the context. When dealing with information and data the important context is, for this article, the system of information. The context is therefore essential to the meaning, the interpretation of the system.[11]

In practice, cybernetics is a relevant theoretical foundation for all systems that deal with control or have objectives[12]. It involves systems that process information since, ultimately, information theory deals with a group of choices[13]. In cybernetics, the choices are messages and the basic units that communicate these messages and the creation of choices in the decision making unit. In warfare it is in this sense especially important that the OODA loop[14], developed by renowned modern warfare strategist John Boyd, is a decision-making process consistent with the cybernetic system[15].

There are four types of information[16] in the cybernetic system: (1) the input of the receptor, the stimulation into the system (message): for example ear and speech (a question), (2) the information stored in the system, input processing and interpretation of information in the decision making unit (interpretation of the message): the brain[17] and memory[18], (3) the output of the effectors, for example answering and producing speech in the speech organs, stimulating the system (message): the ears of another human, and (4) feedback for the control of the system: negative or positive. Feedback is a channel to influence and control the system. Through the feedback, the system does not need to adapt to the changes in the environment, but it can by itself cause change and create its own future[19]. This is a process of transition from being to becoming, from random stochastic change and adaptation to goal oriented and teleological change. For the system to reach a set objective and diminish uncertainty, interpretative information/data is needed as feedback to determine whether a satisfactory answer has been obtained.

Three points form the essence of the cybernetic system. Firstly, the physical matter, the system's structure and its cybernetic parts, and secondly, information/data, abstract differences between the parts of the cybernetic system and within the decision making unit. Thirdly, there is abstract interpretation in the decision making unit which offers alternatives that are produced by processing abstract differences.

There are two categories of cybernetic information: the message coded for the system (input and output) and the interpretation of the message in the decision making unit. What do these two types tell us about cyberwar? The message obviously relates to, for

[11] Bateson (2002), p.13, 16.
[12] Turchin (1977), p.44.
[13] Ashby (1957), p.3.
[14] OODA = Observation (receptor) - Orientation ((into a situation), i.e. decision making unit) - Decision (Output of the decision making unit, i.e. transmitting information to effector) - Action (i.e. effect)
[15] Skyttner (2005), p.416, 417.
16 Skyttner (2005), P.81-85, 91, 92 & Turchin (1977), P.25, 44 & Wiener (2000, originally 1948), P.42, 112.
[17] Brains are structure and order that deal with information saved and inputted by the receptor (Maturana & Varela (1998), p. 22, 34, 126). Corresponding structures that process information are cells and microprocessors (computers). The decision making unit that processes the information from the receptor, interconnects the receptor and effectors and broadens the behavioral possibilities (Maturana & Varela (1998), p.163). To broaden is almost the same as to enable the control of more complex situations (environments and systems).
[18] The short-term memory in the brain is the chemistry of the neurons and long-term memory is permanent connections between neurons, structure within the brain (Teema kanava, 2010). Memory is an instrument that transports information between the past and the future (Wiener, 2000, originally 1948), p.121).
[19] Aula (1999), p.103.

example, communication systems and electronic warfare. What about the interpretation of the message? An essential part of warfare is the understanding of the opponent's activity and interpreting the data collected during reconnaissance. In deception it is important to understand the reasoning of the system being deceived, how it interprets and processes messages and via processing reacts to the relevant message. Only by understanding the level of interpretation can a deception be successful.

Information as the Glue of Organizations

The cybernetic system itself is a basic example of information as the glue of organizations in which receptory data, decision data and feedback data integrate the receptor, the decision making unit and the effector into a single system. According to the inventor of cybernetics, mathematician Norbert Wiener, it is specifically the communication between the parts of the organization that makes a unit intelligent, even if it consists of simple parts, for example, honeybees and ants[20]. His groundbreaking work on cybernetics from 1948 maintains that it is the capacity to access, utilize, retain and disseminate information which holds organisms together. In relation to the above, Wiener lists the printing press, books, newspapers, radio, telephone, telex, mail, theater, film, school[21] and church as vital for large human organizations. Interestingly, Wiener considers that the secondary objectives, such as earning money by using the above mentioned instruments, threaten the unity of the system, which is the primary mission of these communication channels[22].

When the size of the organization grows beyond the possibilities of its information technology, new means for acquisition, utilization, storage and dissemination are needed. This is why language, writing, printing and global computer technology are so important in the evolution of humanity and how they have made the growth of the human organization possible[23].

The Eight Forms of Cyberwarfare

Information-intensive warfare, that is, cyberwar can be divided into four categories[24]. The basis for the division are, first, the actors, which can be the physical person or the physical computer and, second, the operational environment in which the options are physical and virtual reality. Physical reality can be further divided into two parts: first, into physical cyberspace (computers and their intercommunications) and, second, into other types of reality, for example, terrain, people, weapons, constructions, etcetera. Virtual reality signifies a reality created by data (software), for example, the world of a computer game or a detail in a virtual computer-generated car in a racing game. Virtual reality is divided into virtual cyber reality and other virtual realities. There are *eight groups of cyber- or information-intensive warfare*:

[20] This is also central in regards to network-form activity and network-centric warfare. The intelligent operation of the dispersed parts requires their intercommunication! The "network" is not enough!
[21] Okkonen (2002a).
[22] Wiener (2000, originally 1948), p.156, 160, 161.
[23] Ahvenainen (2011), p.124-133.
[24] Ahvenainen (2003), p.23-24, 31.

1. Hacker warfare in which the human and human knowledge are the actors and physical cyberspace is the operational environment.
2. Command and Control warfare in which human and human knowledge are also the actors, but the operational environment is physical reality.
3. Computer network warfare in which the computer and its software are the actors and the operational environment is physical cyberspace.
4. Automated warfare in which the computer and its software are also the actors but the operational environment is physical reality.
5. Simulated hacker warfare in which the human and human knowledge are the actors and the operational environment is virtual cyberspace.
6. Simulated Command and Control warfare in which the human and human knowledge are the actors and the operational environment is virtual reality.
7. Simulated computer network warfare in which the computer and its program is the actor and the operations environment is virtual cyberspace.
8. Simulated automated warfare in which the computer and its program are the actors and the operational environment is virtual reality.

It is worth noting that, generally speaking, Command and Control Warfare is the only one of the eight types of warfare mentioned above that existed before computers. Hence, the computer has made warfare significantly more complex from this perspective. It is also interesting to note the proportion of simulation warfare.

The Human Being as a Cybernetic System and as the Object of Cyberwar

The senses are the most important receptors of the human cybernetic system, the brain is the decision making unit, and the muscles are the effectors. The human is "programmed" by the environment. According to the cybernetic model, there are two possibilities for influencing human beings. First, through the actual[25] message and, second, through programming, that is, by changing the interpretation of the message. The delivery of the actual message can be called narrative[26], transmitting a message, telling the truth, advertising. Hostile activity can be considered distortion of the truth, lying, provocation, propaganda, manipulation and psychological (intelligence?) operations. Sending the actual message requires that the sender has good inside knowledge of the targeted person or group. For example, intimidation can paralyze the target or cause it to react with enraged resistance. Since the human is obviously an extremely complex information processing system, even the evaluation of a single message is a very difficult task.

Another way of influencing people is to program human beings, to change their models of reality. The capacity to create new permanent models of reality makes the impact more reliable and widespread for the actor. If this is carried out extensively and over an extended period of time, it can be called habituation, teaching, training or adaptation. If it is a hostile activity, it can be called brainwashing, propaganda or psychological (intelligence?) operations. The new paradigm of war is strategic communication, proactive and continuous influences

[25] An actual message is a message that first transmits the intention of the sender as intended and then creates the intended actions of the sender in the recipient.
[26] Siren (2011), p.81.

during peacetime dealing with the mind as both the weapon and the main target, putting traditional military means of influence into question[27]. In order to program the human, the human environment must be accessed. Therefore, in regard to Internet, the following additional conclusion is important. Internet is part of the new environment of humanity and it is therefore a source for the programming of human beings and, for instance, an enabler of the above mentioned strategic communication.

World renowned professor, sociologist and researcher of the information society Manuel Castells notes that for human structures the most fundamental form of power is the power to shape the human mind. This is the main hypothesis in his book *Communication Power*. Not only does one need to understand messages and their transmitter, one must also understand how people and organizations process messages.[28]

The Computer as a Cybernetic System and the Target of Cyberwarfare

As a cybernetic system the receptors of a standard computer are, for example, the keyboard, the mouse and the Internet connection. The microprocessor is the decision making unit. Among the effectors are the monitor, speakers, Internet connection, printer and DVD drive (and burner). The computer is programmed by human beings. According to the cybernetic model, there are two ways to influence a computer: firstly, through the actual message and, secondly, through programming, that is, by changing the interpretation of the message.

An example of a message sent to a computer is a keyboard or a mouse command to start a program, to make a selection from within a program, or to feed input. A message can also be disguised as something else, for example, a program can be disguised as an email. Messages can be sent to a computer by a human being or by another computer. A human being can be a system administrator with extensive access, the main user of the program, a regular user of the program, or an outsider pretending to be one of the aforementioned.

The interpretation of a message in a computer emphasizes the importance of the microprocessor, the physical structure of the decision making unit, and the program/software, that is, the rules for processing the message. Therefore, the "deception" of computers requires the understanding of both parts. In theory, the computer software should perform actions that its users want it to perform. In practice, the software does exactly what its code (settings) commands it to do[29]. The same thing applies to integrated chips. *The core of information war or cyberwar lies in this "small" difference*.

Data security expert and physicist Tsutomu Shimomura of the San Diego Super Computer Center, who took down Kevin Mitnick, the most wanted cybercriminal of his time in the United States, has noted that in data security (and in cyberwarfare) it is essential to know how to disassemble the relevant digital locks into parts and to fully understand these parts[30]. The same thing can be said about military systems guided by computers in relation to perceived and real performance.

[27] Siren (2011), p.12-15.
[28] Castells (2009), p.3-4.
[29] Libicki (2009), p.xiv.
[30] Shimomura & Markoff (1996), p.11, 42, 114.

Understanding leads to the control and manipulation of the system, consistent with the Stuxnet virus. The abstract difference (bit) of the computer guiding the physical system leads the system to influence the real physical world through the computer's interpretation. The idea and its implementation are older than Stuxnet[31].

In order to program a computer one has to become part of the group of people programming the computer. These include the manufacturers of the software and those who know how to change the computer's software or install new programs.

The manufacturing of hostile, manipulated integrated chips is called "chipping"[32]. DARPA in the United States is developing a system for recognizing these integrated chips.[33] A corresponding problem regarding hostile code exists in software (programs). The decoding and analysis of software is known as reverse engineering. Antivirus companies are professional analysts of software dealing with the aforementioned problem.

A hostile integrated chip may also be unmanipulated and hence built solely for hostile activity. It is hidden into the complexity of the system's hardware. Examples of these types of integrated chips are key loggers, which record keyboard access and transmit this data to the installer of the integrated chip.

An interesting aspect of computer technology and cyberwar is that in 1986 Unix developer and cryptography expert Robert Morris became the chief scientist at NSA[34], one of the most secret intelligence organizations in the United States. Morris had the knowhow of breaking into computer systems and protecting them.[35]

These problems and the related insecurity and complexity are also the central problem of traditional military performance in the cyber age[36].

Computers already have a long history as targets in cyberwar. Military historian Michael Warner who is specialized in the US intelligence operations lists the following as the decades of cyber[37]:

1. 1960s: Computers can spill sensitive data and must be guarded
2. 1970s: Computers can be attacked and data stolen
3. 1980s and 1990s: Computer attacks can be added to the military arsenal
4. 1990s: Others might do this to us – and possibly already are

The significance of computer technology in the information age is emphasized by the fact that the computer is also an instrument for controlling the complexity, and it opens up the world of complexity to human beings as the telescope opened up the cosmos and the

[31] Shimomura & Markoff (1996), p.59.
[32] Lewis (1997).
[33] http://www.darpa.mil/Our_Work/MTO/Programs/Integrity_and_Reliability_of_Integrated_Circuits_(IRIS).aspx (3 August 2012)
[34] The NSA (the National Security Agency) is the US signals intelligence organization and the security organization for US security officials' computers and telecommunications networks (Warner, 2012, 788 - 9).
[35] Shimomura & Markoff (1996), p.10.
[36] In principle this has not changed. In the book The Egyptian by Mika Waltari, which describes the era of the Pharaohs, the Hittites' horses were fed fodder that was contaminated and the Egyptians won the battle (Waltari, 1982, 690 and 693). Controlling the center of military power has always been the objective of military leaders.
[37] Warner (2012), p.782.

microscope the microcosmos[38]. Computers are also widely used cybernetic components that control almost all infrastructures of society which exposes an unprecedented vulnerability in conflicts[39].

This relates to CIP and CIIP, that is, critical infrastructure protection and critical information infrastructure protection. It is essential to note that information and power are increasingly intertwined. Soft power is gaining ground from old material-based power[40].

Cyberspace: the Noosphere

Information is always connected to a corresponding physical system, the data to be transmitted, the interpretive data and the effect of data. Which of these refer to Internet? Longtime American information and network-centric warfare researchers John Arquilla and David Ronfeldt propose in their book *The Emergence of Noopolitik – Toward an American Information Strategy*, that there exists (1) Internet, the physical structure, the system, its (2) infosphere, and (3) the interpretation of data, the noosphere. However, in their theory, the "infosphere" is composed of cyberspace and media.[41]

The cybernetic interpretation used by the author requires that both Internet and cyberspace are based on (1) the physical structure of the physical system, cyberspace, (2) the transmitted data and other types of data (infospace), and (3) the interpretation of the data in the decision making unit (the noosphere).

From the perspective of cybernetics the noosphere, the dimension of the mind, consists of interpretive information and structures in computers and human beings who add meaning or significance. The noosphere is the central objective of the strategic communication proposed by Arquilla and Ronfeldt.

On Warfare and Cybernetics

In warfare, obvious counterparts can be found to the basic components of the cybernetic system: reconnaissance, command (plus staff and/or command posts), and subunits or, for example, use of force. The objective is central in the leadership in war. At its core, warfare is a goal-directed, information/data processing cybernetic system that transmits messages and makes choices. This is true on many levels: in combat technique, tactics, operations and strategy. In turn, this means that cybernetics as a science is *only one* noteworthy scientific theory for studying warfare, *one* Popper-inspired tentative theory. Since we are living in the era of the information society, this observation is especially important.

The new technological and artificial dimension of information made possible by information technology is a global application of cybernetics. The basic dimensions of existence and warfare have traditionally been time and surface (land and sea) and limited use of space. Earlier, corresponding new dimensions made accessible through technology have been

[38] Pagels (1989), p.42, 309-330.
[39] Warner (2012), p.796.
[40] Arquilla & Ronfeldt (1999), p.ix.
[41] Arquilla & Ronfeldt (1999), p.4, 10-15.

unlimited use of space (aircraft, spacecraft etcetera) and the unlimited electromagnetic spectrum in addition to limited use of light[42]. In this sense, cyberwar is a technological product, a part of a technological evolution that, for example, Professor Eero Paloheimo discusses as a recent and central stage of evolution in his book *The Megaevolution*[43].

In the global dimension of information, cyberwarfare is also the new global level of warfare. Historically, tribal warfare relates to the birth of speech, while state-level warfare relates to the development of writing and lastly, the cultural level of warfare relates to the development of the printing press[44]. By its basic nature cyberwar is global, as is the technology it is based on, for example, Intel, Microsoft, Nokia and Cisco or information services such as GPS, Google, Facebook, Twitter, email and blogs. In its global form cyberwar can exist only as civil war, because by definition only a global mankind exists on Earth. In its global form cyberwar also changes all other lower dimensions of war down to the level of the individual – like all earlier changes have done.

The dimensions considered important in information warfare – the physical dimension, the information dimension and the cognitive dimension[45] – are also obvious cybernetic interpretations. The physical dimension refers to the cybernetic system as a physical structure and as influential on the physical world; the information dimension refers to the transmitted and interpreted data as difference; and the cognitive as the interpretation in the decision making unit. In the above mentioned work, knowledge has been erroneously placed in the information dimension from the cybernetic viewpoint. In the cybernetic interpretation, it is the first phenomenon in interpretative data, the cognitive level.

The main question of the information age is whether warfare is killing and destruction or general hostile activity as, for example, violence. Violence in this interpretation is only one way to achieve the objective of warfare, to coerce the enemy to do our will or the equivalent. Clausewitz says that "*war is nothing but a duel on a larger scale, in which violence is a means and the objective is to compel our opponent to fulfill our will by rendering the opponent defenseless, which is the objective of war*"[46]. The research question of the information era is the following: is violence the only way to coerce the enemy to our will? Whatever the case, the coercion of the enemy to our will adopts the cybernetic interpretation well: Clausewitz's "to fulfill our will" is cybernetically "our interpretation, accepting our message." The message generated with violence is: Surrender!

In around 500 BC The Chinese military strategist Sun Tzu put it in even clearer terms. Firstly, "{a]ll warfare is based on deception," that is, the ability to change the interpretation of the enemy. Secondly, "the best thing of all is to take the enemy's country whole and intact; to shatter and destroy it is not so good." Thirdly, "to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the supreme excellence." Hence, violence is not supreme but the ability to change the opponent's interpretation is.[47]

---

[42] Grabau (1986).
[43] Paloheimo (2002), p.122-154.
[44] Ahvenainen (2008), Wright (1942), p.29-33, 37.
[45] Alberts; Gartska; Hayes & Signori (2001), p.11. Nevertheless, the book in question does not mention the word "cybernetics" or any of its derivatives.
[46] Clausewitz (1998), p.15.
[47] Sun Tzu (2005, originally around 500 BC), p.64, 72-3.

The Soviet Union made a decision in 1969 to copy the computer technology of the West, because it was falling increasingly behind in that area. The only things not copied were the military supercomputers.[48] In the 1980s this decision turned out to be a catastrophic mistake. The Soviet Union was toppled or its toppling was helped significantly by information operations by the United States, used in the 1980s to deliver the best possible Western computer technology and integrated chips, programs and ideas from other areas. All of these later became defective by design.[49]

On this basis, there is one answer to the question of whether violence is the only means of war. If the "Cold War" is defined as a war, it was won by other means than violence. At the same time, it was the first information war and not the Persian Gulf War in 1991 as commonly proposed.

The purpose of information warfare in the 1992 policy was, according to commander in chief Colin Powell, cybernetically interpreted, to remove (decapitate) the enemy and its connections to its subunits.[50] In addition, all types of attacks against communications are based on the previous point, a distinct cybernetic interpretation: to prevent the joint operation of the parts of the system, to destroy them as a system "with minimal effort" by focusing only on communications. After all, cybernetics is the study of the *relationship* of the subsystems in space and time.

Conclusion and New Problems

Cyberwarfare is in this article studied only from one chosen perspective and within a limited number of pages, although the cybernetic perspective can be considered generally significant in the analysis of cyberwar. From the perspective of cyberwar this article is just a part of a greater whole, for example, of this book and its other articles. This should be kept in mind if the article is to be applied in cyberwar, its understanding or as a basis for the formulation of cyberwar related theory.

Cybernetics played a significant role in the author's previous article[51] and in the conclusion it was considered to be a good starting point for further research. This assessment was confirmed in this article. Further studies may reveal why cybernetics does not appear on a wider scale in research or as a theoretical basis for warfare, although an effort was made in this article to highlight its importance. According to Popper one should always start with existent theories, preferably those that have been most widely tested[52].

The classification of cyberwarfare or information-intensive warfare proposed earlier by the author was specified in this article through cybernetic interpretation. In addition to the physical person, the physical computer is another actor, not an abstract computer program. This statement is taken into account and it serves as proof that information/data is always physical and based on a physical system.

---

[48] Susiluoto (2006), p.152-155.
[49] Reed (2004), p.266-270.
[50] Warner (2012), p.790.
[51] Ahvenainen (2011).
[52] Popper (1979, Revised), p.55.

An interesting problem in the article is what can be said about cyberwar[53] in regard to cybernetics. The following can be stated based on this article. First, in condensed form: the new paradigm of warfare of the global era is strategic communication and the new stage of war in the global era is the worldwide web.

In addition, the following can be stated. In the article, old ideas have been connected from Sun Tzu and Clausewitz to the foundations of cybernetics and new interpretations. It is interesting that the latter cybernetic principles are not suggested as a theoretical basis for analysis. The traditional views on warfare, which are briefly introduced by Clausewitz and Sun Tzu, have clear cybernetic contexts. *Warfare is therefore a cybernetic, goal-directed and information processing process or system*. From the viewpoint of cybernetics and warfare this can be considered at least minimally significant.

The eight logical forms of cyber or information-intensive warfare divided by actor and operational environment are hacker warfare, Command and Control Warfare, computer network warfare, automated warfare and the four corresponding forms of simulation warfare. Only one of these existed before computers.

Cyberwar is based on cybernetics. In cyberwar and cyberspace, the essential elements in regard to information are first the messages and then their interpretation.

The message and the interpretation of the message exist both for the human being and the computer. The computer is programmed and the human being becomes "programmed" via his or her environment, slowly through genes and culturally rapidly via memes. The growing importance of the computer is central to cyberwar. It can even be said that global computer technology is the new cyberwar that forms the new emerging model of the new global level (of warfare). The principal model of explanation means that wars taking place in a certain time cannot be understood without the understanding the relevant model of explanation. The computer-related argument mentioned above is supported by the fact that for human beings, cyber (information) has existed as long as the mankind itself.

The difference between the interpretation of the perceived message and the actual message is the core of cyberwarfare or information warfare. For the individual, the perceived interpretation of the message is that the transmitter has a "clear" idea of the meaning of the message and even partly what should take place on the basis of the message. The actual interpretation is what is actually created in the recipient. Professional leadership and basic understanding of cybernetics is to recognize this difference and to act accordingly. The corresponding difference in programs is the distinction between ideal and hostile code, that is, a virus, a worm or a Trojan. The corresponding difference in integrated chips is the difference between ideal integrated chips and hostile integrated chips (chipping). These problems and the insecurity and complexity involved form a central dilemma in traditional military performance in the cyber era.

With respect to computer-based systems, the difference between a perceived and actual interpretation of a message is a central problem and a factor of insecurity in today's military performance. Do we really know the content of military systems? Do we know what the

[53] An interesting problem following this is to ask what can be said generally about warfare on the basis of cybernetics.

integrated chips of military systems really contain? Do we know what the software of military systems really contain?

Generally speaking, cyberwar is a part of the evolution of humanity, warfare and the complexity of warfare. Correspondingly, airspace, outer space and the electromagnetic spectrum have also become parts of warfare.

Cyberwar is based on the enormous efficiency of computer technology. If we cannot affect the new computer-based systems of the armed forces, we are dangerously vulnerable in traditional warfare. If computer-based devices and programs cannot be disassembled into parts and the connections between the parts understood, one is at the mercy of the manufacturer of the device and its program. This makes the control of complexity the core activity in contemporary warfare and society.

By its basic nature cyberwar is global, as is the communication- and computer technology it is based on. As with similar technological advances in the past, cyberwar also changes other lower levels of war.

Cybernetics interpreted through Popper is one of the tentative theories in the study of warfare. This conclusion is especially significant if we observe that data, information, knowledge, and understanding (etcetera) are an increasingly important part of warfare in this (information) era. Cybernetics is also important in warfare and its study since it offers a single integrated theory and a systematic perspective of warfare. Popper's process of evolutionary induction which was used as the foundation of the article should give birth to new problems, which are as follows:

1. Is violence, as according to Clausewitz, the only way to render the enemy defenseless or is warfare general hostility, for example, through violence? Cybernetically understood *violence is just a message* that tries to bend the opponent to our will, to accept our interpretation: the war has been lost.
2. Is cybernetics an underrated theoretical point of departure for research of warfare and information theory? If so, why?
3. Relating to the previous point: what can be said about warfare in general terms, not just in relation to cyberwar?
4. Should cyber and information dimensions be defined by cybernetics, with cyberspace as the physical structure of the information system and the information dimension as abstract differences to be processed, communicated and stored in the aforementioned physical dimension? This view highlights the difference of physical material and abstract information.

References

Ahvenainen, S. (2011). Informaatioteknologia ja ihmiskunta - systeeminen ja evoltutiivinen tarkastelu [Information Technology and Mankind – Systemic and Evolutive Point of View]. In M. Laakkonen; S. Lamminpää; & J. Melaprade, *Informaatioteknologian filosofia* (pp. 113 – 138). Rovaniemi: Lapin Yliopistokustannus.

Ahvenainen, S. (2008). Sotilasfilosofi Quincy Wright ja sodankäynnin muutos – Informaatioajan evolutiivinen ja systeeminen näkemys sodankäyntiin [Military Philosopher Quincy Wright and the New Paradigm of Warfare –Evolutive and Systemic Point of View of the Information Era Towards Warfare] In *Tiede ja Ase 2008* (pp. 134 – 159). Suomen sotatieteellinen seura.

Ahvenainen, S. (2003). Verkostosodan historia ja käsitteen muodostuminen [History of Netwar and the Birth of the Concept]. In M. Piiroinen (Toim.), *Verkostotaistelu 2020 – Taustatutkimus Maavoimien Taistelun kuvat 2020 tutkimukseen* [Network Battle 2020 – A Background Research into the "Maavoimien Taistelun kuvat 2020" Research Project] (pp. 12 – 42). Helsinki: Edita Prima Oy.

Alberts, D. S.;Garstka, J. J.;Hayes, R. E.;& Signori, D. A. (2001). *Understanding Information Age Warfare* (PDF (internet) p.). CCRP Publications Series.

Arquilla, J.; & Ronfeldt, D. (1999). *The Emergence of Noopolitik – Toward an American Information Strategy.* Santa Monica: RAND.

Ashby, R. W. (1957). *An Introduction to Cybernetics.* London: Chapman & Hall Ltd.

Aula, P. (1999). *Organisaation kaaos vai kaaoksen organisaatio? Dynaamisen organisaatioviestinnän teoria [Chaos of Organization or Organization of Chaos –Theory of Dynamic Organizational Communication].* Helsinki: Loki-kirjat.

Bateson, G. (2002). *Mind and Nature.* Hampton Press, Inc.

Bateson, G. (1973). *Steps to an Ecology of Mind.* Paladin.

Bertalanffy, L. (. (2003 (originally 1968)). *General Systems Theory – Foundations, Development, Applications.* New York: George Braziller.

Castells, M. (2009). *Communication Power.* Oxford: Oxford University Press.

Clary, D. E. (1988). *The Bekaa Valley - A Case Study.* Maxwell AFB: Air Command and Staff College – Air University.

Clausewitz (von), K. (1998). *Sodankäynnistä [On Warfare].* (H. Eskelinen, Transl.) Art House.

Gleick, J. (2011). *The Information – A History – A Theory – A Flood.* New York: Pantheon Books.

Grabau, R. (1986). Sechs Dimension des Krieges; Versuch einer analytischen Betrachtung. *Soldat und Technik* [Six Dimensions of Warfare – A Trial for Analytic Examination], Part I: 5/1986 pp.224 – 249, Part II 6/1986 pp.328 - 337 and Part III 7/1986 pp.392 – 398.

Kotilainen, S. (21 Oct. 2012). *Sodankäynnin uusi näyttämö on internet [The New Arena of Warfare is the Internet].* Retrieved on 26 September 2012 at http://www.tietokone.fi/uutiset/sodankaynnin_uusi_nayttamo_on_internet

Lewis, B. C. (Jan. 1997). *Information Warfare*. (Federation of American Scientists (FAS)) Retrieved on 18 Aug. 2012 at http://www.fas.org/irp/eprint/snyder/infowarfare.htm

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar* (Adobe pdf p.). Santa Monica: RAND Corporation.

Maturana, H. R.; & Varela, F. (1998). *The Tree of Knowledge – The Biological Roots of Human Understanding.* London: Shambala.

Okkonen, T. (21. Lokakuu 2002 b). Uudelleenkasvatus tekee vihollisista vaarattomia [Re-education Makes the Enemy Harmless]. *Helsingin Sanomat*.

Okkonen, T. (2002 a). *Yhdysvaltojen näkemykset, suunnitelmat ja toimenpiteet Japanin koulujärjestelmän uudistamiseksi 1942–1947 [The Views, Plans and Actions of US to Renew Japan's Education System 1942–1947].* Oulu: University of Oulu.

Pagels, H. R. (1989). *Dream of Reason – The Computer and the Rise of Sciences of Complexity.* New York: Bantam Books.

Paloheimo, E. (2002). *Megaevoluutio* [The Megaevolution]. WSOY.

Popper, K. R. (1979 (Revised)). *Objective Knowledge – An Evolutionary Approach.* Clarendon Press Oxford.

Reed, T. C. (2004). *At the Abyss – An Insider's History of the Cold War.* New York: Ballantine Books.

Shimomura, T.; & Markoff, J. (1996). *Takedown – The Pursuit and Capture of Kevin Mitnickin, America's Most Wanted Computer Outlaw – by the Man Who Did It.* New York: Hyperion.

Siren, T. (Ed.). (2011). *Strateginen kommunikaatio ja informaatio-operaatiot 2030* [Strategic Communication and Information Operations 2030]. Helsinki: National Defense University – Department of Leadership and Military Pedagogy.

Skyttner, L. (2005). *General systems theory – Problems, perspectives.* World Scientific.

Smith, J. M.; & Szathmary, E. (1995). *The Major Transitions in Evolution.* Oxford University Press.

Sun Tzu. (2005 (originally c. 500 BC)). *Sodankäynnin taito* [The Art of Warfare]. (M. Nojonen, Transl.) Tampere: Gaudeamus Helsinki University Press.

Susiluoto, I. (2006). *Suuruuden laskuoppi – Venäläisen tietoyhteiskunnan synty ja kehitys* [The Arithmetic of Greatness – The Birth and Development of the Russian Information Society]. Helsinki: WSOY.

Teema kanava, Y. O. (2. (8:55 am). Apr. 2010). Documentary. *Muistia etsimässä* [In search of memory].

Turchin, V. F. (1977). *The Phenomenon of Science - a cybernetic approach to human evolution* (Adobe Reader, pdf p.). (F. Brand, Transl.) New York: Principia Cybernetica Project.

Waltari, M. (1982). *Sinuhe egyptiläinen II* [The Egyptian II]. Juva: WSOY.

Warner, M. (2012). Cybersecurity – A Pre-history. *Intelligence and National Security, 27* (5), 781 – 799.

Wiener, N. (2000 (originally 1948)). *Cybernetics: or Control and Communication in the Animal and the Machine* (10 (1. edition 1948) p.). Cambridge (USA): MIT Press.

Wright, Q. (1942). *A Study of War.* The University of Chicago Press.

The Emperor's Digital Clothes: Cyberwar and the Application of Classical Theories of War

Jan Hanska

Abstract

This article uses theories from classical military thinkers to argue that while cyberwar is something new in itself, it does not have to be part of any revolution in military affairs, but rather a sign of normal evolution. War always reflects the characteristics of the societies waging it. Nomadic community provided us with Genghis Khan, industrial societies created mass armies, and the contemporary information society gives birth to cyberwarriors. Existence of war remains the only constant, as do the theories and principles that govern it. The ideas of the classical thinkers need to be restudied, deconstructed, and applied in the new contexts. Ways and means become altered, but war itself remains perpetually a part of the human condition.

Keywords: Cyberwar, Classical Theories, Conventional War, Nordic Cyber.

Cyberwar – Revolution or Evolution?

> "to-day we are faced by so rapid a development, or evolution, […] that this development constitutes a revolution which renders our existing art of war obsolete, so obsolete that unless we can grasp what it portends, to rely on it in another war is likely to prove a greater danger than to enter it totally ignorant of military values."[1]

These words apply to the situation and the hype concerning cyberwar, infowar, netwar – or any other neologism that threatens to overwhelm military strategy and tactics today. Therefore, it should be noted that they were written by J.F.C. Fuller seventy years ago. He saw the military world as tip-toeing on a razor-blade between the past and the future. Fuller argued that tanks and mechanized troops were the decisive factor that would alter the ways and means of war for the future. "As the weapons of war change, so does the character of war change, and though this is an undoubted fact, tactically it must not be overlooked that weapons change because civilization changes"[2] Since we currently live in a computerized and networked world, "so will the wars of this age take on a similar complexion, because military organization follows civil organization."[3] As of yet, cyberwar looms in the future. Cyber attacks as isolated incidents are taking place on a daily basis, and certain concentrated but relatively limited attacks occur every now and then. Nevertheless, a total roll-out of cyber capabilities has not yet been evidenced. We must still try to decipher what is likely to come. Some guidance for this attempt has been offered by Sir Basil Henry Liddell Hart who wrote that

[1] Fuller (1943) p. 7–8.
[2] Fuller (1943) p. 9.
[3] Fuller (1943) p. 9.

> "the future is moulded by the past. The best promise for the future lies in understanding, and applying, the lessons of the past. For that reason […] more light may come from tracing the whole course of the revolution in warfare than by dealing merely with the appearances of the moment."[4]

Be it revolution of mere evolution, the past has led to the present and the seeds of the future are sown today. It is not enough to take today as our point of origin and attempt to draw a line to chart the course into tomorrow. The past has to be taken into account, and since war has been an omnipresent part of the human condition throughout history and pre-history, all lessons paid with blood should not be cast away. We should not solve analog problems with digital solutions.

Heinz Guderian, the famous German Panzer-General, wrote in his memories that while technicians undoubtedly lie, their fables are exposed within a few years if their fantasies do not fit the reality. Tacticians lie as well, but their ideas will be proved false only in a new war, and by then it is too late.[5] Amidst all hype about cyberwar it is necessary to bear the aforementioned point in mind. Our computer-whizz-kids in their eagerness to appear as "Neuromancers" may indeed exaggerate the capabilities of cyber weapons. This is not a serious threat. We must embrace cyberwar, but as strategists, tacticians and technicians we should not let our imagination soar so high that our feet will leave the ground. What we need is not a rejection of the new means to fight wars, but a sombre assessment of how they could be employed as part of our arsenal. "Each new discovery, each new invention, by modifying the forces of peace modifies the force of war. The soldier must understand these modifications, because in the next war they will confront him as actual conditions."[6] Peace modifies war. Therefore, the military organization must stay abreast of those currents and megatrends that shape the peacetime condition of the society, and mould and modify its methods to be compatible with those of the society it belongs to. Yet, one must not rush onwards to the future heedless of the present. We should not create our army anew, and build it from scratch to respond to cyber threats. Once again I resort to Fuller for advice:

> "a new idea should not necessitate a sudden change in structure. Structure can of course be changed, but only slowly, and, in war, if it be rapidly changed, the control and maintenance of an army may be detrimentally affected. Generally speaking, novelties must be limited to work within the existing organization; in other words, a brilliant idea will prove even dangerous unless it can be applied without necessitating a rapid and radical structural change."[7]

In our frenzied search for means to defend our societies, we should not cast aside the tested and true "hardware" of the past, and try to arm ourselves merely with the software of cyber weapons. We need to hold the structures of national defence intact and merely complement them with whatever means are required to defend the cyberspace as well.

As Carl von Clausewitz wrote, "one cannot conceive of a regular army operating except in a definite space."[8] This is true, but the definition of both "space" and "regular army" must be rethought to fit this argument in the context of cyber age warfare. Contemporary army

[4] Liddell Hart (1946) p. 76.
[5] Guderian (1956) p. 29.
[6] Fuller (1926) p. 187.
[7] Fuller (1926) p. 103.
[8] Clausewitz (1989) p. 109.

can no longer consist of "Rambos", and an increasing number of specialists in information technology are needed to conduct a full-scale war. At least, we need to adjust the image of Rambo in our imagination. The "Cyber-Rambo" of today is not pumped with steroids to muscular perfection – he may be an acne-riddled juvenile or a nerdy adult with an enhanced capability for computerized action. We need to understand that the increasingly complex world we live in is mirrored in the way societies conduct their military operations. The contemporary soldier cannot be cast in such a simple stereotype as Rambo exemplifies. An enormous diversity of skills, ranging from the physical to the psychological and to the cognitive, are required in each specified task the soldier has to fulfil. Already Charles de Gaulle noted that

> "Modern conditions of military action demand, therefore, constantly increasing technical skill from fighting men. The equipment, which the force of events has introduced into the ranks, demands the gift, the taste, the habit of serving it. This is a consequence of evolution, ineluctable in the same way as the disappearance of candles or the end of sundials."[9]

It is a fact that throughout history every consecutive generation of soldiers has had to master more complex weapons than the generation preceding it. Likewise, it has to be noted that the acceleration of progress in the computer age has been exponential. Moore's law states that the number of transistors on integrated circuit doubles every two years. The more silicon chips there are integrated into our weapons, the higher are the demands for their users. The pace of progress is something to be marveled at, but lest we accelerate our tempo of adaptation we are likely to fall behind. Every weapon is only as good as its user. Thus soldiers from our information societies, where youngsters are crafty with the latest IT products, have an edge over the soldiers of under-developed countries.

Despite numerous misunderstandings concerning Clausewitz, he still remains a crucial military thinker who should be studied more thoroughly. Numerous definitions of war, and not without contradictions, can be found in his text, but one of the essentials is his claim that "war is thus an act of force to compel our enemy to do our will."[10] His famous maxim that war is the continuation of politics by other means should also be read in this light. War is the ultimate means to coerce the enemy to submission, and it should be used only when diplomatic, economic, political and all other means have been exhausted. There is nothing new in this, since already Machiavelli, who has gained ill fame for his realist views, wrote that "it is better to subdue an enemy by famine than by sword, for in battle, *fortuna* has often a much greater share than *virtú.*"[11] Viewing battles as the playground for fortuna and virtú brings us closer to such contemporary thinkers as James Der Derian. He has argued that the Western way of warfare, perhaps because of the ideas of spreading "democratic peace" through "humanitarian intervention" in many crises demands legitimation, has ascended to a "higher" plane than before. In warfare, it has always been necessary to try to eliminate the significance of *fortuna* for the outcome and to rely solely on one's *virtú.* Der Derian writes that the virtual aspect of war that cyber and computer technology has brought about has become "virtuous." [12] There is an attempt to reinsert the moral weight of the original words and qualities of virtue onto the battlefields, which were initially stripped of

[9] De Gaulle (1976) p. 53.
[10] Clausewitz (1989) p. 75.
[11] Machiavelli (1965) p. 202.
[12] Der Derian (2001) p. xiv-xv.

these qualities, with the technological means of destruction. At the core of the virtuous war lies "the technical capability and ethical imperative to threaten and, if necessary, actualize violence from a distance – *with no or minimal casualties.*"[13] The idea of virtual and virtuous war is to distance war from the dying soldiers and civilians, but even Der Derian admits that, ultimately, "in the final analysis that it seeks to evade, virtuous war is still about killing others."[14] Virtuality, a quality inbuilt into cyberwar, creates with the help of technology and by distancing the battlefield from those operating on it the illusion of bloodless war. Moreover, it attempts to recast cyberwar as a more virtuous way of fighting and, especially, a way without casualties.

What if we are in a situation, in which the entire concept of war has to be, if not rethought, then at least reformulated? If everything in our society has changed due to the increasing speed of progress, and it has been decades since we last had to wage war, is there anything that can guide us for a war of the future? Again, it is Fuller who may provide us with an answer.

> "Is there then nothing permanent we can hold on to? Fortunately, "yes", the principles of war; and directly it is realized that these principles form the foundation of mechanized warfare, just as they do of muscular warfare, it will be seen that revolution is really evolution. What we are faced with is not a new type of war, a war totally unrelated to the present type, but a new form of war, a form arising out of the petrol engine which has greatly enhanced carrying power."[15]

We are not contemporaries of Fuller, and the novelty of mobility provided by the petrol engine to Fuller does no longer enthral our visions of future wars. The form of our future war arises from those factors that have influenced our societal development. In the contemporary world, motorization is old news. Petrol engine has been replaced by the computer as the driving force of the society. A precious insight into war of the future could perhaps be gleaned from the doromologic work of Paul Virilio, whose entire research history is concerned with speed. He has written how

> "just after technological speed, after railways and aircraft, comes absolute speed and the passage to electromagnetic waves. […] But today with video and television, the speed is absolute. We are at the foot of the wall of speed. We are confronted by this wall of the speed of light, we have reached the limit of acceleration, according to relativity. It is a great historical event. The cybercult is a cult to the absolute speed of electromagnetic waves, which convey information."[16]

From mechanization and motorization we have passed into the realm of computerization and networked societies, where even warfare is characterized by the concept of absolute speed of the cyberworld. Yet, following Fuller who was cited above, cyber has not necessarily brought about a revolution. It is true, in a sense, that the Industrial Revolution changed the world, but at the same time entire societies were left behind. The Agrarian Age persisted and existed simultaneously with the Industrial Age. No matter how drastic the change seems to be, a huge part of the "revolution" brought about by the development of computers is still simple evolution. Computers themselves did not bring about a sudden change. Yes, they

[13] Der Derian (2001) p. xv. Italics in the original.
[14] Der Derian (2001) p. xvii.
[15] Fuller (1943) p. 16.
[16] Paul Virilio, cited in Der Derian (2001) p. 65.

were used to calculate how to transplant an astronaut to trample the lunar surface. However, at the time the computational capability was smaller than what we use today to snap silly shots with our smartphones. Computers have evolved with an astonishing speed, and this rapidity makes the evolution look like a revolution.

Before a true revolution can take place, something unquestionably new has to be brought into existence. As a new weapon on the battlefield, gas, and chemical warfare in general were something that could have initiated a revolution, but they did not. Fuller has written about petrol engine and radio as the two real revolutionary factors that altered the way of war like not even gunpowder was able to do.

> "The first not only led to a revolution in road transport and consequently in land warfare, but by solving the problem of flight it raised war into the third dimension. Whereas the second virtually raised it into the fourth; for to all intents and purposes the wireless transmission of energy annihilated time as well as space. Thus two new battlefields were gained – the sky and the ether – the one to be dominated by the airplane and the other by the radio."[17]

Prior to the development of flight, the battlefield was two-dimensional. Flight and its applications added a third dimension. The technical ability to control the electromagnetic spectrum merely added a new element into the 3D battlespace. Cyberspace, again, is the result of enhanced ability to manipulate the aforementioned spectrum. Everything began with the radio as the first means to operate in the "ether". Ultimately the skill of manipulating the entire electromagnetic spectrum did not fully bloom prior to the development of the wireless information networks we enjoy today. All these developments were just extensions of the 3D battlespace and while our world is four-dimensional, it is time and temporality that adds the fourth dimension. No matter how great is the actual battlespace where conventional forces collide or how vast is the infinite cyberspace where network attacks occur, war still cannot exist in an unlimited space. The battle has to have temporal boundaries. The idea of perpetual and omnipresent war is just as inconceivable as Immanuel Kant's idea of perpetual peace. War has to take place in some spatiotemporal context. If the space has indeed extended beyond our comprehension, the idea that a war starts, is carried out, and ultimately ends at a certain point in time keeps it manageable. Choosing where and, especially, when one wants to fight is perhaps the most important decision to be made in initiating war. War can be fought anywhere at any time, but not everywhere and all the time.

Conventional War and Cyberwar – a Bastard Offspring or the Prodigal Son?

At least for the satisfaction of intellectual curiosity, we should still examine the assumed possibility of waging war everywhere and all the time. One of the influential classics of Western philosophy has been Immanuel Kant's *Zum Evigen Friede* which endeavours to realize the utopia of "perpetual peace." At the other end of the spectrum we can find the classic realist writer, Thomas Hobbes, who argued that

> "War consisteth not in Battle only, of the act of fighting; but in a tract of time, wherein only the Will to contend by battle is sufficiently known: and therefore the

[17] Fuller (1946) p. 134.

> notion of Time is to be considered in the nature of War, as it is in the nature of Weather. For as the nature of Foul Weather lieth not in a shower or two of rain, but in an inclination thereto of many days together, so the nature of war consisteth not in actual fighting, but in the known disposition thereto during all the time there is no assurance to the contrary. All other time is peace."[18]

As Hobbes wrote, "all other time is peace" – but what other time remains? States are involved in a deadlock with each other in the worldview of classical realism. War, or, rather a juxtaposition of states in this anarchical struggle, is omnipresent. Cyberwar is a contemporary version of this continuous conflict. Even our rhetoric and vocabulary tend to degrade the meaning embedded in the concept of war. We speak freely of "oilwars", "tradewars" and, for example, the vocabulary of international commerce is often spelled out with militaristic expressions. There is a war between iPhone and Lumia; Nokia, Apple and Samsung are engaged in a "war" on markets. War as a concept has been politicized; it has been devalued and diluted. This applies to cyberwar as well.

One can argue that there are two types of cyberwar. The omnipresent version engulfs us on a day-to-day basis. Our international community, the societies it consist of, the businesses in these societies, as well as the systems of governance are continuously "under attack" – but so are our private laptops. There are innumerable viruses, Trojans, and whatnot prowling through the cyberspace and seeking vulnerabilities continuously. It is only when the attacks become increasingly targeted against particular servers or webpages that we rant about cyber attacks. Nevertheless, it is a fact that while some of these attacks are targeted and purposeful, some are carried out just for a laugh on an almost random basis. This is the omnipresent form of cyberwar. This is something relatively novel and characteristic of our information societies, but what of actual cyber warfare? Today, for a state that starts to trample on its warpath, it would be practically mandatory to include methods of cyberwar as a part of its attack. Then cyberwar is just a part of total war, and its novelty is restricted to being a new weapon of warfare – not a new way of fighting. This is an old trend, since "though military systems also change, war is never annihilated. Except for brief periods of lassitude, the evolution of the weapons and means of war has been continuous and progressive."[19] This creates a situation in which soldiers and military theorists seem to be overwhelmed and dumbfounded. The evolution of weapons in the computerized age has become too accelerated, and "today the basic conditions of war seem to change almost from a month to month. It is therefore hard for the professional soldier to avoid being preoccupied with means rather than ends."[20] Nevertheless, in order to be artists, and not mere artisans, of warfare we must focus our attention and intellectual effort on the ends, but still comprehend the means and their tendency to remain in a flux and develop constantly. As Fuller wrote, "The great genius surges through difficulties immune, because he sees – foresees – the end, and understands the means."[21]

Huhtinen and Rantapelkonen view contemporary wars as paradoxes where, on the one hand, combat is bloodless and computerized. This type of wartime does not differ from

---

[18] Hobbes, Thomas: Leviathan. http://www.gutenberg.org/files/3207/3207-h/3207-h.htm#2H_4_0112. Downloaded 25.5.2012.
[19] Fuller (1946) p. 26-27.
[20] Brodie (1959) p. 16-17.
[21] Fuller (1926) p. 99.

the time of peace. On the other hand, war simultaneously remains a bloody event where people truly die and hence the nature of it has not changed at all.[22] How can we escape the dilemma of this juxtaposition? We need to view warfare as a more complicated issue than two-sided weaponized mass-slaughter. Carl von Clausewitz wrote that "war is an instrument of policy. […] The conduct of war, in its great outlines, is therefore policy itself, which takes up the sword in place of a pen, but does not on that account cease to think according to its own laws."[23] War is a societal aberration, but ultimately it still remains a political tool, "war is simply a continuation of political intercourse, with the addition of other means."[24] According to the realist view of international relations, omnipresent anarchy exists amongst the states that compete for power, influence and prestige. If the states interact in this fashion – as billiard balls colliding against each other – diplomacy, foreign policy, economic policy, and other interrelations between the states do not differ from war. War is just another expression of the thoughts of the state, and "its grammar, indeed, may be its own, but not its logic."[25] War is dictated by the same political purposes that guide all relations between the states that may enter a "war" of economy, a "war" of information, or just as well use the traditional methods of legalized violence in a conventional war. Thus, a state chooses its methods of interaction from a wide variety of means. Traditional diplomacy stands at the one end of this spectrum. Economic sanctions, cyber attacks, and conventional warfare are just grades of escalation when one nears the other end of the spectrum, that is, the total nuclear annihilation of the "mutual assured destruction" policy of the Cold War.

To understand the nature of cyberwar we must cast aside the restrictive dualistic thinking of "war" or "peace" as two absolute and mutually exclusive ontological states. Certain war-like interactions take place during peace and there are peaceful elements in a seemingly "all-out" war. Because of our contemporary technology, a total war between superpowers would leave our globe uninhabitable. A state of war exists on a sliding scale of methods chosen for the purpose of gaining the desired outcome with the least possible use of force. After all, if war in the age of cyber, which we tend to label as "postmodern", is not binary in its nature (that is, we cannot claim that there either IS or IS NOT a war going on as an ontological truth), we must accept the old-fashioned, modernistic idea of Fuller that "[t]here is no intrinsic difference between peace and war, the difference being one of degree."[26] An offensive can be carried out with an aerial strike just as well as with a DDOS attack. Therefore, the classics of strategy and military thought apply also to modern warfare with its additional cyber element. In a sense the tactics of warfare are in a constant state of flux. New attacking methods are developed; counter-measures are invented to curb the destructive potential of the attacking methods; and, again, the human ingenuity creates some other tool of war. The entire concept of cyberwar is merely a new "weapon" to be employed in a particular form of human interaction as old as Cain and Abel. While different weapons require different tactics, the "upper echelons" of human interaction remain unaltered from the level of national policy to that of strategy. Tactics change, but strategic means are a constant. Thus, the principles of strategy remain the same, and it is the task of the political as well as the military leader to apply them in a manner that synchronizes the old principles with the new methods.

---

[22] Huhtinen & Rantapelkonen (2002) p. vii.
[23] Clausewitz (1989) p. 610.
[24] Clausewitz (1989) p. 605.
[25] Clausewitz (1989) p. 606.
[26] Fuller (1926) p. 146.

In many senses cyberwar could be an answer to the agelong dilemma of fighting a war without battles. Sun-tzu wrote that "the one who excels at employing the military subjugates other people's armies without engaging in battle, captures other people's states fortifies cities without attacking them, and destroys others people's states without prolonged fighting."[27] Nevertheless, it is not plausible that future war would be bloodless. If cyber is just another extension of the battlespace, cyberwar is likely to occur simultaneously with more conventional war. We must indeed bear in mind the tendency of war to escalate. Since cyberwar lies at the mellow end of the spectrum of violence, it is likely to commence before kinetic warfare. It will also continue simultaneously with kinetic warfare.

Initiating Cyberwar. Please Wait.

Fuller divided the history of warfare into six time-periods. These are respectively the ages of valour, chivalry, gunpowder, steam, oil, and atomic energy.[28] As we can see, they are not so much rigid taxonomies as descriptions of the prominent characteristic of war during that period. We can view the phase we live in today, for example, as the "age of cyber." It does not mean, however, that cyber would be *the way* war is to be waged in this day and age. It is only one of the means of war, or may even, albeit highly unlikely, to remain a mere open potentiality. Fuller argued that the means to wage war are reflections of the societies that go to war.

> "As the weapons of war change, so does the character of war change, and though this is an undoubted fact, tactically it must not be overlooked that weapons change because civilization changes; they do not change on their own account. To-day wars arise out of economic causes, because our present civilization is an economic one, its master pivot being the machine in one form or another. As the present age is largely a mechanical one, so will the wars of this age take on a similar complexion, because military organization follows civil organization."[29]

Fuller, of course, wrote his text in the industrial age and argued, like many other prophets of future wars, that mechanization will revolutionize warfare utterly. Military organization follows civil organization. Since we in the West have moved from post-industrial societies to knowledge and information societies, it is only natural that our armies explore means to follow the overall societal development. This is achieved by introducing elements of information technology into the conduct of war. Later thinkers seem to agree with Fuller on this point. Heidi and Alvin Toffler have argued that since the force of technology transforms our economy and society, it will transform war as well.[30] How should the cyber weapon then be used? We can look into the past for answers. I would first cite the brains behind the invention of a tank – a new weapon to enter the battlefield in World War I. Ernest Swinton wrote in 1916 that the chance for success

> "lies almost entirely in its novelty, and in the element of surprise, it is obvious that no repetition of it will have same opportunity of succeeding as the first unexpected effort. It follows therefore, that these machines *should not be used in driblets* (for instance, as they may be produced), but that the fact of their existence should be

[27] Sun-tzu (1993) p. 161.
[28] Fuller (1946).
[29] Fuller (1943) p. 9.
30 Toffler, Alvin – Heidi Toffler (1995).

> kept as secret as possible until the whole are ready to be launched, together with the infantry assault, in one great combined operation."[31]

The idea holds water in the context of cyber weapons as well. They have been created in secrecy; nothing is known of their capability; and since counter-measures are relatively quick to develop, it stands to reason that the attack should commence as a surprise, using all possible force at one single instant as part of the military operation as a whole. We may also seek our answer even further back in history. Sun-tzu, the eminent Chinese sage, wrote that "[t]he combat of the victorious is like the sudden release of a pent-up torrent down a thousand-fathom gorge. This is the strategic disposition of force [*hsing*]."[32] Surprise, sudden employment, and full force are factors that need to be present. Cyberwar should not be launched separately from the traditional war but it should be conducted in unison. "[W]hat enable the masses of the Three Armies to invariably withstand the enemy without being defeated are the unorthodox [*ch'i*] and orthodox [*cheng*]. […] one who excels at sending forth the unorthodox is as inexhaustible as Heaven, as unlimited as the Yangtze and Yellow rivers."[33] What was new to Swinton and Fuller (tanks) is now orthodox, and cyberwar offers us the means to employ the unorthodox as part of the total effort to gain victory. "Either-or" is not a formula for success. Victory is only attainable when both the orthodox and the unorthodox are combined seamlessly. The task we are faced with is to create tactics and strategies for operating with cyber weapons as part of the entire military force. In addition, we need to be able to make the weapons interoperable with the other means of conducting operations at our disposal.

As Machiavelli wrote, "[i]f you should happen to be attacked by a regular army, it cannot be so suddenly that you will have insufficient time to put yourself into a proper defensive posture; for such an army must move in an orderly manner, and you will therefore be able to draw up your forces."[34] This remains truer than ever in our information societies. It is impossible for a state to prepare for a conventional attack and keep the preparations secret from the soon-to-be enemy. Cyberwar offers a solution. Since preparations are carried out on computers, "forces" are amassed unnoticed, the chosen targets and the planning of execution seems merely a part of the "business as usual." The surprise element of cyberwar is one of its most prominent characteristics. Contemporary cyberwarriors "remain locked in a standoff for years to fight for victory on a single day."[35] Kaulitya wrote that there are three means of waging war. "Open battle, treacherous battle, and silent battle (*i.e.* killing an enemy by employing spies when there is no talk of battle at all)."[36] I will not enter the discussion about whether a "silent battle" is waged against Iran at the time of writing, or whether being an Iranian nuclear physicist is merely an accident-prone occupation, but cyberwar is easy to place as a new form of "treacherous battle." Some forms of cyberwar, like cyber espionage, can be carried out in the guise of a silent battle. However, if a less limited confrontation between states erupts, Kautilya's maxim is still likely to hold true; "The beginning of an

[31] Swinton (1916) Notes on the Employment of Tanks. Cited in Fuller (1920) p. 51.
[32] Sun-tzu (1993) p. 164.
[33] Sun-tzu (1993) p. 164-165.
[34] Machiavelli (1965) p. 134.
[35] Sun-tzu (1993) p. 185.
[36] Kautilya, Arthashastra, Book 7, Chapter VI, page 15 http://www.sdstate.edu/projectsouthasia/upload/Book-VII-The-End-of-the-Six-Fold-Policy.pdf. Downloaded 7.10.2011.

attack is the time for treacherous fights. "[37] A large scale cyber attack is most likely to occur before the use of air or land forces in order to disable the command and control systems and to disrupt the stability of the civilian society. This is done to maximize the effects of the more conventional means of warfare. We can safely claim that cyberwar is not likely to clear the Clausewitzian fog of war. The fog will remain and create an unpredictable condition of an escalating scale. Cyber weapons do not make war any more "logical" and predictable than it ever was. The main purpose of using them is actually to make the fog even thicker on the enemy so that his scope of vision and his clarity of the situation become more muddled than one's own.

Helmuth von Moltke the Elder wrote in regard to war that "no calculation of space and time guarantees victory in this realm of chance, mistakes, and disappointments. Uncertainty and the danger of failure accompany every step toward the goal, which will not be attained if fate is completely unfavourable. In war everything is uncertain; nothing is without danger, and only with difficulty will one attain great results by another route."[38] Douglas Kellner agrees with the violent, unpredictable and unforeseen characteristics of warfare even today. It has been a somewhat trend in the modern armies to try to counter unpredictability with modern weaponry, mechanized armies, technological organization and hierarchical command structures.[39] In the chaos of the World War II, and of the subsequent wars alike, the failure of modern methods in restraining the pre-historical confusion of war and the fog of war Clausewitz wrote about became evident. The solution offered by the postmodern information societies has been to increase the rationality of the war machine, develop technology, and increase the information flow to and from the battlefield. Paradoxically, the tendency to accumulate and process more and more data in the decision making process has, if anything, hindered the hierarchical structure even more and created a new chaos of abundant and occasionally conflicting information all entangled in a Gordian knot that cannot be unravelled any better than before. The chaotic and confused nature of warfare seems to be unavoidable, and it would be worth once in a while to explore new, or rather, old-fashioned methods to manage the unpredictability instead of always searching for higher and higher technology.

Huhtinen and Rantapelkonen contrast their concept of contemporary asymmetrical information wars or messy wars with the examples of conventional wars, such as the World War I or II. These wars, according to them, were "bound up in a certain place, for a particular purpose and at a given time."[40] But is there a difference after all? It is a question of where one chooses to draw the line between war and "peace-time" politics. Ardant du Picq wrote, with regard to the societies of his time, that "when people become more numerous, and when the surprise of an entire population occupying a vast space is no longer possible, when a sort of public conscience has been cultivated within society, one is warned beforehand. War is formally declared. Surprise is no longer the whole of war, but it remains one of the means in war, the best means, even today."[41] It seems that waging war in the virtual reality opens us, again, the chance to initiate war without a formal declaration of war – and, thus, without a

[37] Kautilya, Arthashastra, Book X, Chapter 3 page 3-4 http://www.sdstate.edu/projectsouthasia/upload/Book-X-Relating-to-War.pdf. Downloaded 7.10.2011.
[38] Moltke (1993) p. 175.
[39] Kellner (2008) p. 17.
[40] Huhtinen – Rantapelkonen (2008) p. 61.
[41] du Picq (1987) p. 72.

forewarning to the enemy. There is no doubt that the weapons of cyberwar are used today even in the most outwardly peaceful relationships between countries.

This brings us to a point argued by Jomini: "War once decided upon, the first point to be decided is, whether it shall be offensive or defensive."[42] All of the Nordic countries have decided upon cyberwar. Our policy, however, seems to be to keep the war defensive. Thus, we build up our protection in the realm of computer-networks and argue that these actions are precautions. However, they can just as well be called defensive operations, because there is no clear dialectic relationship between peace and war in warfare that takes place inside the information technology and in networks. Paradoxically, we can say that in the binary world of computer technology war escapes this binary nature. The state of war and that of peace are not "1" and "0"; instead, they are much harder to determine. In the realm of cyber, the old and often quoted maxim of Vegetius rings true: "He, therefore, who desires peace, should prepare for war."[43] Furthermore, it is not enough to construct a sufficient defensive structure, albeit it remains a necessity. What Stuxnet taught us is that an attack may occur; and if the enemy is a superpower, it is likely to be conducted by means hitherto unknown. In the realm of cyber, offense is the best form of defence and one needs to remain in a status of high alert to commence one's own cyber attack. If cyber is just an initial state of warfare, one has to commence with it since "part of the victory consists in throwing the enemy into disorder before you engage them."[44]

Nordic Cyber

Cyber seems to offer a chance for the small high-tech Nordic countries, since cyber defence would be relatively easy to build up with the aid of such businesses as F-Secure. Unfortunately, the fact remains that our complex, technically advanced and democratic welfare societies belong among the most vulnerable potential targets of cyber attacks. Our societal infrastructure is so dependent on high-speed Internet connections and automated computerized systems that even a short disruption in these functions would cause unpredictable problems to emerge.

Cyber defence is often lauded because it is a relatively cheap capability to build up in the realm of ever-increasing prices of traditional armaments. Nevertheless, creating offensive capability is proportionally just as cheap, and since the Nordic states are small in terms of economic resources (at least, when compared with the potentialities of the superpowers), we will face the same problems as with traditional armaments. The great power will always be superior when push comes to shove, and our societies are even more vulnerable in the realm of cyber than in that of geopolitics. In the latter realm, we should at least know where the battles of the future are likely to occur. On the contrary, there are no maps of the cyberworld to ponder upon and use in our war-gaming. We have wisely chosen to participate in the arms-race of the cyber age; yet, perhaps erroneously, we have also chosen a defensive posture. Clausewitz argued that the "aggressor often decides on war before the innocent defender

[42] Jomini (1992) p. 72.
[43] Vegetius (1985) p. 124.
[44] Vegetius (1985) p. 158.

does,"[45] and thus, "a battle accepted is regarded as already half lost."[46] It is possible that in the realm of cyber the battle has already been completely lost. We need offensive cyberwar capabilities and, unlike the superpowers of the cyberworld, we as small states need to parade our skills and capacity in offensive cyberwar – or more correctly, the potential to carry out an offence. This capability, underlined and continuously developed, can act as the deterrent of the cyber age. If we show willingness to retaliate against a cyber-aggressor, we may be able to diminish the possibility of having to defend ourselves against one. We do not yet know whether we will have any retaliatory capability after falling victim to a massive cyber attack. This only emphasizes one of Napoleon's maxims: "the transition from the defensive to the offensive is one of the most delicate operations in war."[47]

There is no reason to undermine the importance of the entire governmental and societal structure when building up as thorough cyber defence as possible. Nevertheless, the society also needs a capability for cyber attack. It is one thing to protect the smooth functioning of a society, and another thing to prepare for cyberwar. As du Picq argued, "[a] general's ability lies in judging the best moment for attack and in knowing how to prepare for it."[48] Our countries must strictly adhere to the understanding of how to develop our cyber capabilities. We cannot leave the task solely to it-specialists; nor should we try to re-invent the wheel within a group of soldiers. Bernard Brodie wrote with regard to the nuclear weapon that "we cannot go on blithely letting one group of specialists decide how to wage war and another decide when and to what purpose, with only the most casual and spasmodic communication between them."[49] Whatever shape the cyber capabilities of our countries will take, the related skills must be built in close co-operation with all relevant participants from the society. Offensive cyberwar should be under military control. The military, in turn, is controlled by the political establishment. However, cyber defence is a concern of the entire society – individuals, companies and institutions alike. In order to "mobilize" our full development potential we need to include experts from all possible fields in the planning and construction of our cyber capabilities.

If we discuss cyberwar as a factor isolated from the total war that includes the traditional kinetic means of inflicting damage, the old adage of Frederick the Great fits our age: "The effect of surprise would certainly not last long to-day. However, to-day wars are quickly decided."[50] It is likely that cyberwar as part of total war mostly consists of one massive initial strike. When discussing only cyber, war will be quickly decided. Thus preparedness, both in terms of defensive and offensive capabilities, needs to be at a high level. As Jomini wrote: "civilized governments ought always to be ready to carry on a war in a short time, – that they should never be found unprepared."[51]

When planning a cyber attack, one must realize that its effects do not manifest similarly in all societies. There is no use to employ a cyber attack against an undeveloped society – like there is no sense in attacking a small island state in the Pacific with a mechanized component of the land army. The idea of attacking a failed state, like contemporary Somalia, with

[45] Clausewitz (1989), p. 370.
[46] Clausewitz (1989), p. 361.
[47] Napoleon (1987), Maxim XIX, p. 62.
[48] du Picq (1987) p. 162-163.
[49] Brodie (1959) p. 7.
[50] du Picq (1987) p. 132.
[51] Jomini (1992) p. 46.

cyber weapons is ridiculous. Certain tools can only be used to achieve certain ends. Cyber attack should only be directed towards an enemy with computerized functions in its societal infrastructure. An agrarian society would not suffer from a cyber attack nearly as much as a European developed information society. However, this "limitation" in the use of cyberwar does not undermine its effectiveness as long as the target has been suitably chosen. "The arrow shot by an archer may or may not kill a single man; but skilful intrigue devised by wise men can kill even those who are in the womb."[52] There is no telling how widespread the damage caused by an all-out cyber offensive could be before it has occurred in real life.

I am by no means arguing that we should not strive to our utmost in developing the cyber capabilities. On the contrary, we must rush forward and lead the development, as well as embrace all new inventions that influence the way we will fight in the future. Lest we do that, we will be like the generals of the world wars, who, according to Fuller, "could not see that, because civilization was becoming more and more technical, military power must inevitably follow suit: that the next war would be as much a clash between factories and technicians as between armies and generals."[53] Of course, in this citation Fuller was able to use 20/20 hindsight when evaluating the fundamentals of the past wars, but it is easy to predict a similar development to occur a hundred years later. The frenzy of factory production churned out machines of war for the World War II like it produced bullets and rifles for the mass armies of World War I. Both of these wars were characterized by mass production and they indeed took the shape of wars between factories and technicians. Likewise, a contemporary war can be characterized by factors prevalent to the societal structure of our times. We are likely to have a war between information networks and systems. Nevertheless, we should not forget that war, as it proceeds, is not evolutionary. The more time goes by, the further the means and ways of war tend to slip back to the "tested and true". Therefore, even in cyberwars clashes where foot-soldiers fight each other with rifles and bullets will occur – sooner or later. Multiple stages of war will likely take place simultaneously. Perhaps, there will be a war of movement, of attrition, and of cyber. We need infantrymen, tanks, and all other traditional weapons which have not yet been made obsolete – AND we need new cyberwarriors. Along with the new technologies and information systems we must adjust to the idea that neither machines and computers, nor infantry riflemen can by themselves produce solutions to all situations one is likely to encounter in warfare. We need soldiers who are able to fight both in computer-generated information-networks and in networks created by humans among themselves. We need techno-warriors with enhanced skills to function in the economic, social, cultural, political and technological battlefields, as well as traditional "warriors" able to function amid the bloodiest hand-to-hand combats and to counter the "horror" the imaginary Colonel Walt Kurtz whispered about in Francis Ford Coppola's movie "Apocalypse Now".

Nuclear Cyber

There is a defence against almost every weapon. Cavalry was countered by the Roman phalanx. The birth of tanks and their breakthrough in the Battle of Cambrai in the World War I gave birth to anti-tank measures. The predominance of air power resulted in anti-

[52] Kautilya, Arthashastra, Book X, Chapter 6 page 12 http://www.sdstate.edu/projectsouthasia/upload/Book-X-Relating-to-War.pdf. Downloaded 7.10.2011.
[53] Fuller (1946) p. 134.

aircraft artillery and missiles. Every development in armament has its counter-development. Except for one: in the past almost seventy years no antidote has been invented for nuclear weapons, since the current anti-ballistic-missile systems are not reliable enough to gamble for the stakes involved in an all-out nuclear war. Because of the impossibility to protect oneself from the first-strike, a clear analogy between nuclear and cyber weapons can be drawn. There is no more effective means to defend oneself from a nuclear blast than there is to defend from a virus attack. In the case of the latter, the reason lies in the fact that until a particular weapon has been used we are not familiar with any of its inherent qualities and thus, we cannot create a fool-proof defensive system. "A defense is built, and the offense seeks to exploit its weak spots. And the history of the race thus far suggests that there is always a hole, an Achilles' heel."[54] The evolution of "weapons" in cyberwar is hectic and hence describing them is of no use. After all, Stuxnet or Duqu are no longer as effective as they were at the time they were rolled out due to the developed counter-measures. As Machiavelli wrote, "when you are aware that the enemy is acquainted with your designs, you must change them."[55] There is no doubt that future weapons like these have already been developed. Thus, it not so much a question of *what* the weapons of cyberwar are, but *how, where* and, especially, *when* to use them. One of the interesting paradoxes of cyberwar is that weapons can only be used once. Each time a particular strain of virus has been released it is able to fulfil its function only for a limited period of time. One does not have to be the Nostradamus of the cyber-age to predict that the exposed Duqu, Flame, or Stuxnet were versions 1.0 and that version 2.0 of each, or rather *n*.0, is ready to be released. Every computer virus can be employed only once and, unlike conventional weapons, monitoring them is impossible. There is no way of knowing what kinds of virus arsenals are being held in the digital "silos."

To understand the irrational logic of cyberwar one might do worse than to become acquainted with the early nuclear theorists. If there is no plausible defence, the only means of defence is offense. Along this path we are soon involved in the paradox-ridden discussion which one wit of the nuclear age summarized as "I won't attack first unless you do". We resurrect the talk of pre-emptive strikes that would be easier to carry out in this case than in the case of nuclear weapons. After all, cyberwar is not "real war", and we uphold an illusion that the digital bombing of an advanced and networked society back to a digital stone-age – or a Commodore 64 age, if you will – could be carried out without casualties. The paradoxical nuclear strategy has been born again. When probably outdated viruses (deemed so from the focal point of their creators) like Stuxnet and Duqu have been let loose, these have been probing attacks. Should a war break out between two advanced states with cyber capabilities, the initial attack is likely to take the form of digital *Blitzkrieg*. Since one's capability to manipulate the cyber realm is dependent on his or her computer networks and the systems being intact, one has to release full offensive capability before the opponent has time to initiate his or her own attack. The age of cyber is likely to roll out the resurrection of total war. After all, even a civilized, humanitarian nation is able to morally justify an unrestrained cyber attack due to the illusion of bloodlessness and because there is no code of conduct or international law regulating cyberwar.

Since at least Clausewitz, Moltke the Elder and von Schlieffen, who was fascinated by the performance of Hannibal at Cannae, there has been a strong fascination with the idea of

[54] Brodie (1959) p.202.
[55] Machiavelli (1965) p. 203.

"battle of annihilation". This has gradually developed into visions of a total war where all powers of a nation state are harnessed for military purposes. The idea of total war fell out of favour by being too successful in the totally devastating World Wars. It was a maxim of Helmuth von Moltke that "[r]apid conclusion of a war undoubtedly constitutes the greatest kindness. All means not absolutely reprehensible must be used to accomplish this end."[56] However, the atomic age taught mankind a lesson. An all-out unrestricted warfare with every means at the superpowers' disposal could no longer be considered an option. As Fuller wrote,

> "'Total warfare', such as we have known it hitherto, is not compatible with the atomic age. Total warfare implies that the aim, the effort and the degree of violence are unlimited. Victory is pursued without regard to the consequences. […] An unlimited war waged with atomic power would make worse than nonsense – it would be mutually suicidal."[57]

Nonetheless, just as old drunks find it hard to stay on the wagon, the hawkish contemporary thinkers seem to have found their hair of the dog in cyberwar. Many of the theories of early nuclear thinkers apply to this form of warfare – excluding those of mutual suicide. Cyberwar seems to promise the fulfilment of the illusion of total war without bloodshed, as well as unlimited power without retaliation.

There is a profound similarity between nuclear weapons and cyber weapons. This resemblance is most striking when one considers the characteristics of the earliest atomic bombs and the latest cyber weapons. All repercussions of a nuclear attack were not properly understood before they were put to use. The side-effects included both radiation and nuclear fallout. The "father" of the atomic age, Doctor Oppenheimer, claimed that nuclear weapon is "a weapon for aggressors and the elements of surprise and of terror are as intrinsic to it as are the fissionable nuclei."[58] Similarly, we should not lull ourselves into the belief that in cyberwar mere defensive measures would be enough. "We have to remind ourselves again of the great military advantage of striking first in a total war"[59] The importance of seizing the initiative is explained by Bernard Brodie; "unless we can strike first and eliminate a threat before it is realized in action […] we are bound to perish under attack without even an opportunity to mobilize resistance."[60] Stuxnet, Duqu and Flame are comparable to the test explosions in the deserts of New Mexico, and the full potential of cyber weapons is yet to actualize. Nevertheless, we must not despair and envision a cyber attack that would devastate all our computer systems with a single stroke. The future of cyberwar remains undecided and the direction its development will take is unclear. Brodie, Kahn, and the other early nuclear strategists wrote with the same enthusiasm as all major theorists writing after the World War I who were touchingly in unison concerning the role gas would play in future war. Yet, in large quantities the utilization of gas on battlefields has been fairly limited. Does this then mean that Fuller, Liddell Hart, Guderian, or Triandafillov were mistaken about future weapons?[61] Indeed, they were not. The international community just perceived the method

[56] Molke (1993) p. 24.
[57] Liddell Hart (1950) p. 377.
[58] Oppenheimer, Robert. Cited in Brodie (1946) p. 73.
[59] Brodie (1959) p. 354.
[60] Brodie (1946) p. 72.
[61] For a very interesting vision of warfare see Triandafillov (1994), whose main argument was that the western theorist who emphasized small high-tech armies was erroneous. Triandafillov advocated mechanized million-man armies and his vision grounded the Soviet theory of war for a long period of time.

of gassing soldiers and populations alike too inhumane and therefore, banned the poisonous gas as a weapon. True, there have been relapses, like the US in Vietnam and Saddam in the Middle East, but these have been rather isolated incidents than mass uses – unlike the theorists predicted.

Military thinkers have their own warped logic concerning what is humanitarian in warfare. Moltke wrote that the ultimate kindness of a commander-in-chief lies in using massive force. He argued that "rapid conclusion of a war undoubtedly constitutes the greatest kindness. All means not absolutely reprehensible must be used to accomplish this end."[62] The mind is abhorred by the idea of using force so that all of it is spatially and temporarily concentrated. It is a frightening prospect to release the pent-up force and allow it to rampage unrestricted. Why this nonetheless should be done is because surprise has always been accepted as a powerful force multiplier. Catching the enemy off guard increases vastly the damage inflicted. As Guderian, who caught France with her metaphorical pants down, wrote,

> "Surprise may hang upon the very novelty of the weapon in question. It takes considerable daring on the part of a commander to use a weapon for the first time, but in the event of success the rewards will be all the greater. We have seen, however, that neither the Germans with their poison gas nor the British with their tanks were willing to accept the risk of employing new weapons *en masse* in a surprise attack. Once the fleeting opportunity had been missed, surprise could depend only on the kinds of time-honoured techniques which had been used with the conventional weapons. Even then, however, there remained a considerable scope for catching the enemy off guard."[63]

Someone will seize the initiative in cyberwar as well. This brings the element of surprise into the battle. Being the first is risky, but having made that choice it is likely that the attack will be massive, because, as Clausewitz wrote about surprise and seizing the initiative, "they are infinitely more important and effective in strategy than in tactics. Tactical initiative can rarely be expanded into a major victory, but a strategic one has often brought the whole war to an end at a stroke."[64] If the cumulative effects of an all-out cyber attack do not disrupt the targeted society severely enough, more conventional armed force is needed for the subsequent military action. By spending more on cyber, one can create huge savings in blood and lives. The viral "warriors" of the cyber age are cheaper to send into battle than their human counterparts. I do not suggest that conventional force would not be used, since boots are always needed on the battlefields, but the resistance they are likely to encounter can be decimated by cyberwar. The strategy and the tactics of cyber age are still intoxicated by the notion that war could be fought and won with a single decisive surprise attack. This age-old dream of a war decided in one attack was crystallized by Moltke in his time: "The modern conduct of war (Kriegführung) is marked by the striving for a great and rapid decision. Many factors press for a rapid termination of the war: the struggle of the armies; the difficulty of provisioning them; the cost of being mobilized; the interruption of commerce, trade, business, and agriculture."[65] Cyber weapons offer an illusion of a digital lightning strike that would be so devastating that the enemy could not respond with traditional methods of warfare before its will has already been broken.

[62] Molke (1993), p. 24.
[63] Guderian (1992) p. 75-76.
[64] Clausewitz (1989) p. 363.
[65] Moltke (1993), p. 176. See also p. 125.

Should we then fear a digital Armageddon? Has the old Doomsday clock of the nuclear scientists now taken a digital display and is ticking seconds to annihilation? My answer, again, is no. Liddell Hart argued convincingly that "war experience teaches us that no new weapon proves so deadly in practice as in theory – a lesson which corresponds to the wider truth of human experience that nothing looks either so good or so bad in retrospect as it appeared in prospect."[66] So far, at least by the time of writing, we have not witnesses a cyber attack on a level that could be reasonably labelled as "war." In theory, cyberwar has the potential to annihilate the entire global networked community and therein is its strictest limitation. It is hard, perhaps impossible, to perform truly devastating, yet targeted cyber attacks. Internet is not a tube through which one could send a digital "bomb" and limit the scope of destruction precisely to the target. Its networked nature does not allow this. Destruction proceeds along the net and it has its repercussions. It is implausible that a superpower, say, the U.S., would attack China with all its cyberarsenal to wreak havoc on China's entire economic system, because the collapse of China's markets would bring about a financial collapse in the U.S. as well. Stock exchanges of the world are too interlinked. One needs to take the networked structures into account when planning his or her attack and, consequently, one will have to limit the scope of the attack right from the initial stages onwards. Again, in the words of Liddell Hart, "while there is reason to doubt whether the new robot weapons will ensure a quick decision, it is probable that they will multiply the general destructiveness of war, and the extent on useless damage caused to all parties."[67] Cyberwar could turn out to be even more damaging to the civil society than the mass bombings of German cities in World War II or even the butchery and slaughter Gaius Julius Caesar led when conquering Gaul.

At the moment, cyberwar is in a peculiar limbo. It is not yet regulated by international law, humanitarian laws, intergovernmental agreements, or any other institutionalized means. These are some of the main factors that, according to Clausewitz, "tame the elemental fury of war."[68] Cyber is the one and only aspect of warfare in which possibilities at one's disposal are as yet unlimited. This situation is likely to silence the doves and set the hawks screeching. Cyber seems to offer the chance to fight beyond the jungle of restrictions and regulations that covers conventional warfare. Furthermore, since everything concerning cyber capability can be hidden, building the offensive capability and preparing for a massive attack can be made in secrecy, and even the origin of the attack, once it occurs, can be obscured, it seems like a plausible scenario that we will need to witness a full-scale attack before any limitations of cyberwar are created. We need to see to believe. It is beyond the scope of both me and this article to even try to predict the forms attacks are likely to take, but that is not a major setback. Any computer virus so far programmed, any weakness waiting to be exploited is inconsequential, because the rapidity of progress is so accelerated that by the time these words find their reader any techniques outlined would, in all likelihood, have already become obsolete. With regard to cyberwar, in this lull before the storm, what needs to be addressed is the philosophy of this new form of waging war – and not its weapons. Even today the words of Sun-tzu ring true: "Warfare is the greatest affair of the state, the basis of life and death, the Way [Tao] to survival or extinction. It must be thoroughly pondered and analyzed."[69]

[66] Liddell Hart (1946) p. 33.
[67] Liddell Hart (1946) p. 33.
[68] Clausewitz (1989), p. 218.
[69] Sun-tzu: (1993) p. 157.

I find close connections between the philophies of nuclear war and cyberwar. In retrospect, it is amazing that nuclear weapons remained a part of the strategic, operational, and even tactical arsenal of the superpowers throughout the Cold War. Nevertheless, it is a promising thought that despite the advice and demands of certain generals, nuclear weapons were not used in Korea or in Vietnam. Perhaps Homo sapiens is fitting description for our race after all. It remains a historical fact that the only open war between two nuclear powers has been that of India and Pakistan, and this was confined and limited to small factions in the Siachen glacier and certain parts of Kashmir high on the Karakorum mountain range. It was not an all-out confrontation. During the Cold War the nuclear arsenals of both superpowers allowed armed animosity to break out between them only by proxy. Wars were fought by other players in the countries of the Third World, but with considerable assistance of both superpowers. Nevertheless, the possibility of nuclear war remained minuscule. Even when a superpower attacked a small state, the fear of nuclear intervention by other superpowers kept nuclear weapons off the battlefield. This was mainly due to the aversion towards and the universal moral condemnation of the use of these weapons. Now, if we take a leap into the future of cyberwar, the possible scenario is similar in the following respect: it is unlikely that the future cyberpowers would risk attacking each other for the fear of a massive retaliation, if there is even a remote possibility that the origin of the attack could be deciphered, because the financial cost of the damages could be astronomical. Thus, cyber deterrence is practically effective already. The difference is that, since there is no universal ban on cyber weapons, the states that do not have sufficient cyber capabilities remain potential targets. This applies to the "pariah-states" of the international community, like North Korea or Iran, just as well as to any other state that a cyberpower wants to coerce. The cyberpowers are likely to remain untouchable as long as it is possible to identify the state that has been the assailant, but the small states enjoy no other protection than the defence they build.

Coda

I have written about the massive and combined use of cyber weapons, because it would be the most effective way of using them. Like in classical strategy, when all force is focused on one point, and employed at the right time and in simultaneity, its effects become multiplied. Thinkers, as removed in philosophy and temporality as Moltke and Kautilya, are in unison with regard to the use of force. The former wrote that "everything available must be thrown into battle at all circumstances, for one can never have too much strength or too many chances for victory."[70] The latter echoes this idea from antiquity, claiming that a commander-in-chief "should march with his full force; otherwise, he should keep quiet."[71]If one wants to use cyber weapons to pressurize the enemy government, harassment and partial use would be a sound strategy. If one chooses to carry out a war, all possible force should be employed for that purpose and, furthermore, this should happen in an instant, single moment. Liddell Hart's words describe cyberwar well: "The explanation may be found in the natural fact that decisive results come sooner from sudden shocks than from long-drawn pressure. Shocks throw the opponent off his balance. Pressure allows him time to adjust himself to it."[72] However, as in war in general, we cannot argue that cyberwar

[70] Moltke (1993), pp. 128-129.
[71] Kautilya, Arthashastra, Book IX, Chapter 1 page 1 http://www.sdstate.edu/projectsouthasia/upload/Book-IX-The-Work-of-an-Invader.pdf. Downloaded 7.10.2011.
[72] Liddell Hart (1946) p. 25.

would be a binary concept, that is, that it would either be ongoing or non-existent. There are many forms of cyberwar, starting from the everyday industrial espionage and gradually escalating along the spectrum of offensive cyber measures. This applies to conventional war as well. Even Clausewitz, the proponent of massive and concentrated force, wrote that it is possible to "reduce war to something tame and half-hearted. War is often nothing more that armed neutrality, a threatening attitude meant to support negotiations, a mild attempt to gain some small advantage before sitting back and letting matters take their course."[73] Our contemporary military vocabulary includes terminology like "operations other than war" or "low-intensity conflicts" that describe the less severe ways of using institutionalized violence which armies represent. The form of cyberwar I have mostly been discussing is the total war: hard to defend oneself from and one likely to inflict massive damage. Simultaneously probing exploitations of weaknesses and limited data-thefts find their slots on the spectrum, and it is easier to build defences against these measures. Nevertheless, if one plans how to defend one's assets, it does not suffice to prepare for less than the biggest threat. What good is a Kevlar west that would offer protection only from plastic bullets? If we want to be credible cyberwarriors, we need suitable defensive and offensive capabilities. If one decides to build a hammer, in order to use it effectively it should not be made of marshmallow. "We live in extraordinary times, in days of strange and violent possibilities. Daily war is becoming even more a struggle between inventors than between soldiers."[74]

My main argument is that there is no need to laud the death of Mars or any other god or goddess of war. *Le roi est mort, vive le roi* still remains the way to proceed when pondering on the relationship between war and human condition. The age of mass armies composed of infantry died with the World War I, the mechanized mass army with the World War II. Out of the ashes of every war rises the phoenix of the next war. The king or the emperor remains in charge, albeit his or her name changes. The actual person – or the means of warfare – may have died, but the institution remains. We should not hasten to imagine that the new version would be something totally alien to the past. The war of today or tomorrow will certainly look different. In its outward aspects, it may even be different from the wars of the past, but the foundational principles will remain the same. We should not be distracted by the new digital clothing of the emperor, but cast ourselves into the role of the child who saw the emperor naked and likewise penetrate the veil of cyber and virtuality that tends to obscure the bloody and murderous primal nature of war. Even in cyberwar, people are going to die – and there is nothing virtual and often not even anything virtuous in those deaths. Our international system has grown more and more complex, and even its centres of gravity and sources of power seem to fluctuate. The Westphalian system of the nation states as crucial and ONLY actors in the realm of international politics belongs to the past. New actors have emerged and everything is networked, interlinked, and yet fluid. However, this only applies to the advanced societies. The underdeveloped countries are not able to "enjoy" the freedom and ambiguity of post-modernism. Indeed, they remain dead-locked to modernity or even to pre-modernity. As all these actors try to figure out their interrelations, wars are likely to keep erupting and these wars are likely to bear all characteristics of the societies participating in them. Thus, we may find cyberwar and industrial, even agrarian warfare existing alongside each other. These wars may not be only "messy" but chaotic. When our cyberwarriors of tomorrow look for guidance in their operations, I propose searching the

[73] Clausewitz (1989) p. 218.
[74] Fuller (1946) p. 155.

past for answers. After all, it is practically impossible to deny the truth Kautilya wrote in his Arthashastra in the 4th century B.C.; *"striking in all places and at all times, and striking by surprise are varieties of waging war with infantry*."[75] Attacking in all places, all times, and with the aid of surprising strikes can function as a guideline for planning over two millennia later. It is just as applicable to the tools of cyber as to those of foot-soldiers. Kautilya further argued that success in war depends on a certain trinity. "*Strength, place, and time, each is helpful to the other*."[76] The sum of these factors determines the outcome of the battle. Each must be supportive to the others and their balance must be carefully calculated.

References

Brodie, Bernard:. Implications for Military Policy. In *The Absolute Weapon – Atomic power and World Order*, ed. Bernard Brodie. Harcourt, Brace and Company, New York, 1946, pp. 70–107.

Brodie, Bernard: *Strategy in the Missile Age*. Princeton University Press, Princeton, 1959.

Clausewitz, Carl von: *On War.* Edited and translated by Michael Howard and Peter Paret. First paperback edition, Princeton University Press, Princeton, 1989.

De Gaulle, Charles: *The Army of the Future*. Greenwood Press, Westport, 1976.

Der Derian, James: *Virtuous War – Mapping the Military-Industrial-Media-Entertainment Network*. Westview Press. Boulder, 2001.

du Picq, Ardant: Battle Studies – Ancient and Modern Battle. In *Roots of Strategy*, *Book 2*, Stackpole Books, Harrisburg, 1987, Pp. 65-300.

Fuller, J.F.C.: *Tanks in the Great War 1914-1918.* John Murray, London, 1920.

Fuller, J.F.C.: *The Foundations of the Science of War.* Hutchinson & CO (Publishers) LTD, London, 1926.

Fuller, J.F.C.: *Armoured Warfare – An Annotated Edition of Fifteen Lectures on Operations between Mechanized Forces*. Eyre and Spottiswood, London, 1943.

Fuller J.F.C.: *Armament and History – A Study of the Influence of Armament on History from the Dawn of Classical Warfare to the Second World War.* Eyre & Spotiswoode, London, 1946.

Guderian, Heinz: *Sotilaan Muistelmia*, Org. Erinnerungen Eines Soldaten. Transl. Wolf H. Halsti. Kustannusosakeyhtiö Otava, Helsinki, 1956.

Guderian, Heinz: *Achtung – Panzer!* The Development of Tank Warfare. Translated by

[75] Kautilya, Arthashastra, Book X, Chapter 5 page 9 http://www.sdstate.edu/projectsouthasia/upload/Book-X-Relating-to-War.pdf. Downloaded 7.10.2011.

[76] Kautilya, Arthashastra, Book IX, Chapter 1 page 2 http://www.sdstate.edu/projectsouthasia/upload/Book-IX-The-Work-of-an-Invader.pdf. Downloaded 7.10.2011.

Christopher Duffy. Cassell, London, 1992.

Hobbes, Thomas: Leviathan. http://www.gutenberg.org/files/3207/3207-h/3207-h.htm#2H_4_0112. Downloaded 25.5.2012.

Huhtinen, Aki-Mauri – Jari Rantapelkonen: *Imagewars – Beyond the Mask of Information Warfare*. Marshal of Finland Mannerheim's War Studies Fund. Helsinki, 2002.

Huhtinen Aki.Mauri – Jari Rantapelkonen: *Messy Wars.* Finn Lectura, Helsinki, 2008.

Jomini, Antoine Henri de: *The Art of War*, Greenhill Books, London, 1992.

Kautilya: *Arthashastra*. http://www.sdstate.edu/projectsouthasia/upload. Downloaded 7.10.2011.

Kellner, Douglas: The Ideology of High-Tech/Postmodern War vs. the Reality of Messy Wars. Preface in Huhtinen Aki.Mauri – Jari Rantapelkonen: *Messy Wars*. Finn Lectura, Helsinki, 2008, pp- 9-23.

Liddell Hart, B. H.: *The Revolution in Warfare.* Faber and Faber LTD, London, 1946.

Liddell Hart, B.H.: *Defence of the West – Some Riddles of War and Peace*. Cassell and Company LTD. London, 1950.

Machiavelli, Niccolo: *The Art of War*. A revised edition of the Ellis Farneworth Translation, Bobbs-Merrill Company, Inc., Indianapolis, 1965.

Moltke, Helmuth von: *On the Art of War – Selected Writings*. Ed. Daniel J. Hughes, Ballantine Books, New York, 1993.

Napoleon Bonaparte: *The Military Maxims of Napoleon*. Ed. David G. Chandler, Greenhill Books, London, 1987.

Sun-tzu: Art of War. In *The Seven Military Classics of Ancient China*. Ed. Ralph. D. Sawyer, Westview Press, Boulder, 1993, Pp.145-186.

Toffler, Alvin – Heidi Toffler: *War and Anti-War: Survival at the Dawn of the 21st Century*. Warner Books. New York, 1995.

Triandafillov, Vladimir K.: *The Nature of the Operations of Modern Armies.* Translated by William A. Burhans. Frank Cass, Portland, 1994.

Vegetius: De Re Militari, In *Roots of Strategy*, Ed. Thomas R. Phillips, Stackpole Books, Harrisburg, 1985, Pp. 65-176.

Theoretical Offensive Cyber Militia Models

Rain Ottis

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 by 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.

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; thus, volunteering for the cyber front.

Cases like the 2007 cyber attacks against Estonia are good examples of situations in which 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.

Method and limitations

In this article[1], I use theoretical qualitative analysis to describe the attributes, strengths and weaknesses of three offensively oriented cyber militia models. I have chosen the three plausible models on the basis of what can be observed in the context of recent cyber conflicts. The term *model* refers to an abstract description of relationships between the 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 the models in reality or in the examples provided. In reality, it is more likely to see groups that match a model only partially, or combine elements from more than one model. On the other hand, the models should serve as useful frameworks for analyzing volunteer groups in 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).

The Forum

The global spread of Internet allows people to connect easily and form „cyber tribes", which can range from benign hobby groups to antagonistic ad-hoc cyber militias.[2] 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".[3] It serves as a command and control platform where more active members can post motivational materials, attack instructions, attack tools, and so on.[4]

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 that was active in the course of the Russia-Georgia war in 2008.[5]

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:

[1] *This article originally appeared in the Proceedings of the 6th International Conference on Information Warfare and Security, Washington DC, USA, 17-18 March 2011. It has been edited for clarity and format compatibility.*
[2] Williams & Arreymbi (2007), Ottis (2008), Carr (2009), Nazario (2009), Denning (2010).
[3] Ottis (2010b).
4 Denning (2010).
[5] Carr (2009).

web forum, Internet Relay Chat channel, social network subgroup, and so on. 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 its 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.[6] 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, and so on.[7] Some of the Forum members may also be active in cybercrime. 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. Even if there seems to be evidence that a lot of the individuals engaged in such activities are relatively unskilled in cyber attack techniques,[8] when supplemented with a few more experienced members the group can be much more effective and dangerous.[9]

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.[10] However, this still does not allow strong command and control, as each member can decide what, if any, action to take.

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 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 it and there is no lengthy vetting procedure.

[6] Ottis (2010b).
[7] Ibid.
[8] Carr (2009).
[9] Ottis (2010a).
[10] Denning (2010).

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 its members.[11]

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.[12]

Weaknesses

A clear weakness of this model is the difficulty to command and control the Forum. Membership is not formalized and often it is not even 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 an uncontrolled expansion of a 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 by using attack kits or malware.[13] They are highly reliant on instructions and tools from the 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 and 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

[11] Ottis (2010b).
[12] Ottis (2009).
[13] Ottis (2010a).

that have phone-home functionality to the members, and so on. Note that some of these options may be illegal, depending on the circumstances.[14]

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.[15] 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 by Carr.[16]

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, usually in response to a long-term problem, such as the Israel-Palestine conflict. The activity of such 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 cybercrime. For example, with 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.

[14] Ottis (2010b).
[15] Young & Aitel (2004).
[16] Carr (2009).

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.

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.[17] 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.[18] As described by Ottis,[19] it is probably not necessary to actually identify all of 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.

[17] Carr (2009).
[18] Ibid.
[19] Ottis (2010b).

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.[20] The model can be divided into two generic sub-models: anonymous and identified membership.

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 in 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), and so on. 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, and so on) in order to achieve a common goal. The same approach is possible for a cyber militia as well. In fact, Williams and Arreymbi suggest that gaming communities can be a good recruiting ground for a cyber militia.[21]

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.

[20] Krekel, et al. (2009). See also PLA Reserve Forces. Globalsecurity.org. Available at: http://www.globalsecurity.org/military/world/china/pla-reserve.htm [Accessed 17.11.2012]
[21] Williams & Arreymbi (2007).

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.

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 be further 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 it can 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, 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 the role assignments get settled. During this process, which could take days,

months or even years, the militia is relatively inefficient and likely unable to perform any complex operations.

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 human beings, one of the most potent ways to neutralize cyber militias is through information operations, for example, by persuading them that their identities have become known to the law enforcement.

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 the 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 and 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 "peacetime" 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 its numbers and use relatively primitive attacks, the Cell is capable of more sophisticated attacks due to its 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 become more frequent every year. In most cases, 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 identified strengths and weaknesses should serve as useful guides to dealing with the cyber militia threat.

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.

Offensive Cyber Capabilities are Needed Because of Deterrence

Jarno Limnéll

Abstact

Within the next couple of years, the world will experience more intentionally executed and demonstrated cyber attacks. Simultaneously, the development of offensive cyber weapons will become fiercer and publicly more acceptable. As different actors develop more sophisticated cyber capabilities and acquire experience in their use, the picture will grow more complicated and nuanced.

Keywords: Cyber, offensive, deterrence, attribution, credibility, weapons, cyber treaty.

Today, cyber capabilities are essential for the nation states and the armed forces that wish to be treated as credible actors. Cyberspace, the fifth dimension of warfare, has already become an important arena of world politics – especially, since the times of war and peace have been blurred and become the grey area we are currently living in. The nature of cyberreality (the blurring of peace and war) adds a dangerous new dimension of instability: future conflicts may become vague, without a clear beginning and end. Sometimes the actor may not even be conscious of being in conflict with someone, when unpleasant tangible things "just happen" all the time or just every once in a while. The digital world has become a domain where strategic advantage can either be lost or won.

We are Moving toward a Ubiquitous World

It is very important to understand that in the future the difference between kinetic and non-kinetic environments will become ever more blurred and that in many respects these environments will merge into one.[1] Almost everything will be digitally interconnected, and the cyber domain will expand and become more complex. This indicates that the possibilities and means to do things will broaden considerably and that the integration of the cyberworld with the physical world will give a new dimension to human life. Therefore, cyber should not be treated as a separate domain, but as one that is entwined with the physical space.

In military terms this means that modern warfare will demand effective use of cyber, kinetic, and combined cyber and kinetic means.[2] Cyberwar could be an additional domain in traditional warfare or a standalone approach to warfare – both are likely to occur. Cyber operations can be kinetic and/or non-kinetic. Boundaries between conventional and cyber operations are blurring, since cyber attacks begin to be used as a force multiplier in conventional operations.

---

[1] Jurvansuu 2011.

[2] See, as an example, Department of Defense Strategy for Operating in Cyberspace 2011.

It is also essential to bear in mind that cyber attacks can do things that conventional attacks cannot – with devastating and unprecedented effects.

Defence, Resilience and Offense

Even if we would like to think so, success in the cyber domain is not only a question of defence – at least, not for the nation states. Defence capabilities have to be as preventive as possible in order to reduce the effectiveness of the adversary´s – whoever it may be – cyber attack. However, despite the best defensive efforts, intrusions will occur. Therefore, one also has to be resilient in the cyber domain, that is, one has to have the ability to withstand attacks and failures, as well as to mitigate harm more than in other domains. The creation of cyber defence capabilities and resilience are pretty easy for the public to accept. Yet, these acts are not enough. Deterrence is also needed, that is, the capabilities and policies to convince the others not to launch a cyber attack against one. Deterrence will only be effective if one can build and demonstrate offensive cyber capabilities. To put this in a clear manner: offensive cyber capabilities are an essential element for the nation-states to succeed in their current and future international and security policies.[3] Defence, resilience and offense all contribute to the country's overall ability to protect herself – one needs them all.

From Nuclear Deterrence to Cyber Deterrence

The ambiguities of cyber deterrence contrast starkly with the clarities of nuclear deterrence. In the Cold War nuclear realm, attack attribution was not a problem; the prospect of battle damage was clear; the 1,000th bomb could be as powerful as the first one; counterforce was possible; there were no third parties to worry about; private firms were not expected to defend themselves; any hostile nuclear use crossed an acknowledged threshold; no higher levels of war existed; and both sides always had a lot to lose.[4]

Deterrence theory was developed in the 1950s, primarily to address the new strategic challenges posed by nuclear weapons. During the Cold War, nuclear deterrence was able to keep the United States and the Soviet Union in check. Nuclear deterrence was the art of convincing the enemy not to take a specific action by threatening it with an intolerable punishment or an unacceptable failure. The theory has worked well.

Based on that logic, cyber deterrence should play a similar role in the digitalized world. However, anonymity, advantage of attacks, global reach and interconnectedness greatly reduce the efficiency of cyber deterrence. Simultaneously, there is a lot of suspicion and rumours travelling around: what kind of capabilities the others might have and how they are using them already?

In the kinetic world, it is much easier to evaluate the opponent's capabilities. It is quite easy to make a valid estimate on how many tanks, interceptors or submarines a country possesses. Countries also openly expose their arsenal, for example, in military parades, as

[3] Limnéll 2012.
[4] Libicki 2009.

well as their operational skills, for example, by organizing large military exercises. In the logic of deterrence, it is even more important to manifest force than to have real capabilities – yet the others have to know it.

Awareness Prevents Conflicts

Deterrence depends upon effective communication between the state and the entity it wishes to deter. One has to convince the others that if they attack, one has the capability and the capacity to do something about it. This is also the case in the cyber domain. If a country wants to be a credible actor in this domain, it should openly declare its offensive policy and expose its offensive capabilities. The policy acts as the rules for engagement. This is the trend some countries are already moving toward. For example, for the first time since the Second World War, Germany has publicly disclosed that it is developing offensive cyber weapons.[5] In addition, in the latest Cyber Strategy of the United States, offensive cyber policy is strongly emphasized, and it has been said in public that the US Defense Advanced Research Projects Agency (DARPA) is focusing its research on offensive cyber capabilities.[6] It has also been announced by many countries that a response to a cyber attack is not limited to the cyber domain, which is very understandable.

The world needs to start talking openly about offensive cyber capabilities and the readiness levels – just as we discuss missile arsenals, air force, submarine fleets, or doctrines. We talk about great military exercises taking place in the kinetic world, but there is very little public discussion on things happening in cyberspace. Today, countries are aware of and appreciate the kinetic capacities which the others have. This is one reason why there are so few on-going wars in the world. Awareness prevents conflicts – at least, between the nation states – and it raises the threshold for conducting an attack. The defence policy of many countries is based on this assumption – if you have and if you are able to expose strong enough military capability, the likelihood of being attacked decreases.

The Challenge of Attribution

Lately, there has been a lot of discussion about the problem of attribution, which differentiates the logic of warfare in the cyber domain from the other domains. Yes, attribution is hard because it lacks the obviousness of a kinetic attack and leaves no physical evidence. Attacks can also be masked or routed through the networks of another country. Even if one knows for sure that the attack came from a computer in a certain country, one cannot be sure that the government is behind it. It is hard to deter without being able to punish, and one cannot punish without knowing who is behind the attack. Moreover, hitting back to a wrong target weakens the logic of deterrence and also creates a new enemy. This allows totally new players enter the field of warfare which was formerly held solely by the nation states. These players are called terrorists. Cyber terrorists may take an advantage of the situation in which some or very little offensive capabilities exist.

[5] Leyden 2012.
[6] Nakashima 2012a.

Attribution is difficult, but it is not impossible.[7] It requires both technological solutions and diplomacy – and, in particular, wide international cooperation. Communication channels between countries should be created, and to be used when something extraordinary happens in the cyber domain. I am convinced that when countries start discussing their cyber capabilities more openly and admit the existence offensive strategies (which, in any case, are the reality), it will become politically easier to approach the touchy issues of rules and norms in the cyber domain in international cooperation. Where there is a will, there is a way.

At the same time, it has been interesting to notice that in some cases certain actors have willingly claimed the responsibility for conducting cyber attacks. If not doing so, the others would not know it and the actor in question could not take any political advantage of the attacks. This has been the case with Stuxnet. The U.S. government has unofficially admitted the attack in order to take credit for it – just before the presidential elections of 2012. By admitting Stuxnet,[8] the United States also pointed out that she was capable of and willing to use an advanced cyber weapon against an adversary. This is a strong message of deterrence.

Offensive Weaponry is Required for Credibility and Deterrence

Discussion on offensive cyber weaponry should begin. As emphasized, currently there is no credible status for the armed forces and the nation states without cyber capabilities – this includes the offensive capability. The arms race is on and accelerating, even if we would like to turn a blind eye to it. The most frantic contemporary race is about talented individuals. When it comes to the creation of cyber capabilities, the question is not about the number of people one employs but about the talent the employed have. The US, China, Russia and many other countries are actively recruiting promising hackers. So are, most likely, Al Qaeda and other organizations. The real cyber question is about the talent and about creating cyber capabilities with the help of the most talented individuals.

It is not very popular or even desirable to talk publicly about offensive cyber weaponry in most countries. However, it has become necessary to explain the logic of offensive cyber capabilities to the general public. Naturally, this has to be done in various ways in different countries due to cultural and national reasons. The reasons why countries are developing offensive weapons and why they need them can be summarized into the following four points.

First, if one wishes to be a *credible actor* both in the military battlefield and in world politics, one must have offensive capabilities – as one must have defensive capabilities and the ability to be resilient. One simply cannot have a credible cyber defence without offensive abilities.

Second, in order to achieve and *raise her deterrence*, one must possess offensive capabilities. The ability to act offensively includes a strong preventive message to the others – provided that they understand it and believe it. Offensive capabilities represent the key component of deterrence.

[7] Hunker, Hutchinson, Margulies 2008.
[8] Nakashima, Warrick 2012.

Third, offensive thinking and building offensive weaponry are vital in order to *create a strong and credible defence.* With just "defence thinking" one will not succeed. One has to have an understanding of how the attacker acts, and one should try to find all possible vulnerabilities in her own defence. It is also a matter of developing one's defensive potentials, testing the current defence and training one's forces. All this becomes much more efficient if one can test it with her own capabilities. Without the ability to act as an attacker, no country can build an effective and credible cyber defence.

Fourth, agility and the concept of operations for smart defence are reality in contemporary warfare for most countries. One will never achieve her objectives by just being defensive – regardless of how defensive her grand doctrine is. In some cases, as it has been in the past, attack is the best defence. One cannot stay in bunkers. Instead, one has to be an *active defender* and snatch the initiative when it is needed. Passive defence alone will not work. In short, when the lights go off how does one defend with kinetic weaponry against a non-kinetic adversary?

Disclosing Offensive Weaponry Becomes More Visible and Includes Great Risks

One of the biggest challenges and threats today is that countries are secretly developing and using their offensive cyber capabilities. The trend is very worrying. Offensive cyber weapons have already become so sophisticated that they are able to produce major disturbance, as well as paralyze societies´ critical infrastructure.

In every domain of warfare, there is the concept of deterrence which consists of real capabilities, doctrine and the others' awareness of one's capabilities. Merely talking about offensive cyber weapons in general terms, without revealing or even demonstrating these capabilities, will not advance deterrence very much.

Currently, cyberwarfare initiatives often follow the rules of guerrilla warfare. However, this will change soon. As the four-star General James Cartwright has said: "We've got to step up the game; we've got to talk about our offensive capabilities and train to them; to make them credible so that people know there's a penalty to this."[9] Just like with kinetic weapons, one's adversaries must know the weaponry possessed. In order to deter, the nation states must be able to show their capabilities without sacrificing the advantage that surprise may deliver – in defence and in offence.

In the next couple of years, the nation states will expose their offensive cyber capabilities more openly in order to enhance their deterrent effect. The states will demonstrate their capabilities by organizing exercises and simulations which will be openly reported. In addition, the effects of some offensive capabilities will be disclosed. However, most probably this will not be enough.

The nation states are "forced" to conduct cyber attacks in real situations and against real targets. This will mean attacks against terrorist or activist groups, industrial plants, or even

[9] Reuters 2011.

against other states. After conducting attacks, the nation states will claim the responsibility in order to increase their cyber deterrence. As an example, in May 2012 the US Secretary of State Hillary Clinton announced that the agency's specialists attacked sites related to Al Qaeda on which the organisation tried to recruit new members.[10] This was a strong political message of intent to use cyber weapons. It was a glimpse into the future of cyberwarfare – and it served to build credible deterrence.

Naturally, the question of using cyber weapons is controversial. When the nation states and other actors start to increase the use of offensive cyber capabilities, there is always the possibility of escalation. One event can quickly lead to another and an even greater conflict may arise – as the history has taught us. There is also the severe question of unexpected side effects which may occur when releasing cyber weapons. The end result could be, in the worst case, a total darkness of the unpredictable and interlinked digitalized world, even if that was not the original intention. Cyber deterrence within the area of operations may be very difficult to limit.

When the nation states are thinking about the creation of cyber deterrence, they face the aforementioned challenges. Something that is secret cannot be used as a deterrent. At the same time, there is too much detailed information on the weapons' capabilities available, which makes it easier for the adversaries to defend themselves against these weapons, for example, by blocking the vulnerabilities that the weapons exploit. Discussing or demonstrating cyber capabilities too openly would probably accelerate the cyber arms race even more and in ways that might be self-defeating. However, if the adversaries know that the digital infrastructure is resilient; that there is a credible threat detection and prevention system; and that there is a capability to conduct counterattacks, the deterrence is much more credible.

The Need for an International Cyber Treaty

It seems that the cyber domain turns all players offensive. So far, cyber operations have been interpreted as a "softer action", which makes the threshold of acceptability much lower than that of traditional military operations. In online strategy, offense dominates defence. In other words, it is more conducive to attackers than to defenders. This leads to new and complex dimensions in national security policy. There is a real need for the regulation of the digital battlefield agreed on a "Cyber Treaty." Cyber arms verification (identifying and measuring a given player´s offensive capability) is difficult, which increases the possibility of surprises in international relations. The absence of agreed or clear rules and norms, as well as the current imprecise knowledge of the ultimate cause-effect of cyber attacks can leave open ambiguity that leads to escalation. For now, there are no known or tested escalatory logics for a cyber battleground exchange. This begs the question of how far-flung militarization of the cyber domain we will testify.

[10] Axe 2012.

Civilians in the Front Lines of the Cyber Battle

It is important to understand that cyber deterrence cannot be undertaken by a government or an army alone. The general public must also be involved. Civilians are in the front lines of the cyber battle – every day. For example, if a significant number of home computers in a country have no firewall or anti-virus software installed, attackers will exploit these vulnerabilities each day to secretly take over and remotely operate thousands of computers hence turning them into botnets. This turns the nation into an adversary's offence capability and against itself.

The public is a very central point when creating cyber deterrence. It is not only about the importance of increasing the general knowledge about cyber security and the actions that must be done at the individual level. Everyone has a role when a country is trying to create more efficient cyber defence capabilities and to be a more resilient society. This may, in turn, create a totally new chapter in nation state economy and politics.

Countries are building offensive cyber capabilities and will use them more openly. If the general public does not understand the meaning of offense as part of defence, it is much more difficult to use them openly, that is, to strengthen the cyber deterrence. Thus, secret actions will continue, which will lead to much worse results. If the public understands the logic – and the seriousness – of creating offensive cyber weapons, the threshold to use these weapons will most probably decrease, because there will be an understanding of the devastating consequences. However, one will have her deterrence.

References

Axe, David (2012). "Clinton Goes Commando, Sells Diplomats as Shadow Warriors."", Wired 24.5.2012.
http://www.wired.com/dangerroom/2012/05/clinton-goes-commando/

Department of Defense Strategy for Operating in Cyberspace, 2011.
http://www.defense.gov/news/d20110714cyber.pdf

Hunker, Jeffrey; Hutchinson, Bob and Margulies, Jonathan. Role and Challenges for Sufficient Cyber-Attack Attribution, Institute for Information Infrastructure Protection, 2008.

Jurvansuu, Marko. Roadmap to a Ubiquitous World. VTT 2011.

Leyden, John. "Germany reveals secret tecnie soldier unit, new cyberweapons", 7.6.2012.
http://www.theregister.co.uk/2012/06/08/germany_cyber_offensive_capability/

Libicki, Martin C. Cyberdeterrence and Cyberwar, Project Air Force, RAND Corporation 2009.

Limnéll, Jarno. “Suomenkin osattava hyökätä verkossa”, Suomen Kuvalehti 30.9.2012.

Nakashima, Ellen. “With Plan X, Pentagon seeks to spread U.S. military might to cyberspace”, Washington Post, 30.5.2012.
http://www.washingtonpost.com/world/national-security/with-plan-x-pentagon-seeks-to-spread-us-military-might-to-cyberspace/2012/05/30/gJQAEca71U_story.html

Nakashima, Ellen and Warrick, Joby. “Stuxnet was work of U.S. and Israeli experts, officials say”, Washington Post, 2.6.2012.
http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

Reuters, “Ex-U.S. general urges frank talk on cyber weapons”, 6.11.2011.
http://uk.reuters.com/article/2011/11/06/us-cyber-cartwright-idUKTRE7A514C20111106

Threats Concerning the Usability of Satellite Communications in Cyberwarfare Environment

Jouko Vankka & Tapio Saarelainen

Abstract

Satellite communications offer a network system that can be quickly constructed and is deployable relatively rapidly. Moreover, it provides a wide variety of services to military troops in peace supporting and military operations without requiring a land-communications network system. Satellite communications offer a reliable communication gateway and a broad footprint.

The paper begins with a discussion over the international operational experiences of the Finnish Defence Forces. By using the Kosovo Force (KFOR) operation as an example, it provides a perspective into the communications sphere. First, the paper focuses on three possible threats to the usability of KFOR satellite communications systems in cyberwarfare; namely, physical weapons, logical weapons and network attacks. It examines these three threats and proposes methods that are applicable in countering them.

Second, the paper discusses the matter of welfare communications. Welfare communications is an important factor in maintaining morale. Satellite links play an important role in providing phone, entertainment and e-mail services to operational servicemen. Minimizing social media-induced operational security threats requires that at all parties involved in the operation are properly trained for and aware of the constantly present risk in social media communications.

Keywords: Satellite communications; Distributed Denial of Service attack; Man-in-the-middle attack; Welfare Communications, Operations Security

Introduction

Satellite communication is particularly useful in conditions in which traditional communication is difficult or impossible, for example, due to the lack of adequate infrastructure on the ground. This has especial significance for defense. The ability to transmit detailed information quickly and in a reliable way helps streamline military command and control, as well as ensure information superiority. This enables faster deployment of highly mobile forces capable of interoperable, robust, and "network-centric" communications. As of April 2006, the percentage of communications provided by commercial satellites for the Operation Iraqi Freedom was eighty-four percent[1]. Finland does not own satellites. Therefore, communications for the Operation Kosovo Force (KFOR) in Kosovo has been

[1] Steinberger, J.A (2008). A Survey of Satellite Communications System Vulnerabilities. M.S. thesis, Joint Electronic Warfare Center, June 2008.

provided by commercial satellites. The commercial satellite communication has been supplied via leased transponders on-board INTELSAT satellite[2]. Unfortunately, commercial satellites and earth stations are not built with the capabilities to protect themselves from potential attacks, such as physical weapons, logical weapons and network attacks. Such attacks could cause the unavailability of military communications at a critical moment in conflict. Due to the criticality of satellite communications to the Finnish Defence Forces Crisis Management Operations it is highly important to understand the vulnerabilities in satellite communications systems. Understanding these vulnerabilities facilitates the thwarting of the possible attacks against them in the future.

Communications Systems in Crisis Management Operations from 1982 to 2003

This chapter briefly discusses the use of satellite communications by describing international operational communications experiences of the Finnish Defence Forces from 1982 to 2003.[3]

In the United Nations Interim Force in Lebanon (UNIFIL) operation, which was carried out 1982–2001, a High Frequency (HF) radio was utilized. The communications system was insecure, and only able to transmit and receive speech. During the operation, another insecure and unreliable connection was provided through the analogical landline telephone. In this context, voice communications posed the most significant threat to operational security.[4]

In the Stabilisation Force (SFOR) operation in Bosnia and Herzegovina (1996–2003) satellite implementation was utilized for the first time. The communications was provided by SONERA (a Finnish telecommunication company) and it had a bandwidth of 1 Mbs. In case of a need for backup hauling satellite telephones were available. The operational security threat identified earlier remained the same.[5]

When the Kosovo Force (KFOR) operation began in 1999, satellite phones were still used for backup hauling. The connection rate of the satellite was updated to 2M/512Kbs. In addition, the communications system now featured Internet as a new element. Encryption was added. The earth station of the broadband satellite internet implementation was located in FIN NSE (Fyrom). The identified operational security threats arose from both voice and online communications. The end-users of online services were identified as a potential operational security threat in that they might transmit written and visual data in the form of e–mail messages and attachments.[6]

In Figure 1, the transmission of data is categorized as unclassified, classified, secret, Voice over Internet Protocol (VOIP) and video. The DVB-RCS is an acronym for Digital Video Broadcasting – Return Channel via Satellite (or Return Channel over System). It is a specification for an interactive on-demand multimedia satellite communications system.

[2] Vankka (2009).
[3] Vankka (2009).
[4] Vankka (2009).
[5] Vankka (2009).
[6] Vankka (2009).

The DVB-RCS is based on the asymmetry in bandwidth for the broadcasting and returning channel. In the forward direction the data rate is 2Mbs. The return channel data rate is 512Kbs. The earth station sends and receives signals to a satellite in a geostationary orbit around the earth (INTELSAT 10-02 in Figure 1). In the geostationary or geosynchronous orbit 36 000 km above the earth's surface, the satellite completes a revolution in exactly the same amount of time that it takes the earth to rotate a full turn on its axis. At this altitude, satellites appear to be fixed in relation to the earth, therefore the name 'geostationary satellites'. This eliminates the need for satellite dishes at the user location to track the satellite, which greatly simplifies their construction and reduces the cost. The earth station is connected to an Internet backbone, which provides Internet access from any location on earth. Unfortunately, Internet connections are susceptible to a variety of attacks, such as distributed denial-of-service (DDoS), man-in-the-middle attack and other cyber threats. Virtual Private Networks (VPNs) securely connect remote locations through cost-effective Internet access instead of using expensive dedicated wide area network links. In Figure 1, the VPN uses Internet to provide KFOR offices an access to the network of the Finnish Defence Forces. The firewall, again, is used to protect networks from an unauthorized access while permitting legitimate communication pass.[7]

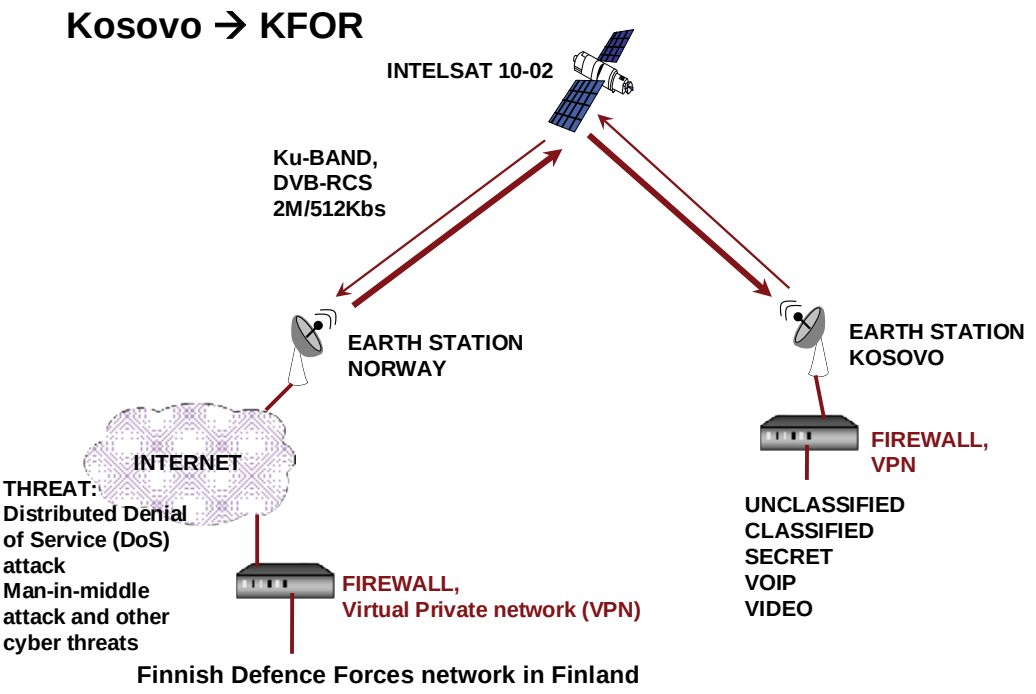


Figure 1. A simplified structure of a communications system used in the KFOR operation.

[7] Vankka (2009).

Satellite Communications Vulnerabilities

This chapter focuses on three possible threats to the usability of satellite communications systems in the cyberwarfare environment; namely, physical weapons, logical weapons and network attacks.

Physical Weapons

Physical weapons can be classified into five categories: physical attacks, kinetic-energy weapons, directed-energy weapons, electronic jamming and hijacking. The weapons are positioned as defensive in nature. However, the same laser that can be trained on a military satellite can easily target a commercial satellite instead.

1) Physical Attacks

The earth stations are susceptible to physical attacks which can potentially wipe out communications across the space system. For this reason, defence forces may need to protect their satellite earth stations by means of basic military force [8].

2) Kinetic-Energy Weapons

Kinetic-energy weapons destroy targets by smashing into them at a high speed9. According to basic Newtonian physics, the impact energy increases linearly with the projectile's mass, but as the square of its impact velocity. Because collision speed is comparable to projectile speed, lightweight projectiles would be sufficiently destructive – assuming they find their target. To understand the destructive power of kinetic-energy weapons, one must consider velocity. A standard military-issue 7,62×39 mm projectile is traveling at 715 meters per second. The orbital speed of the kinetic-energy weapon is from 6,9 km/sec. up to 7,8 km/sec. depending on the altitude. Satellites consist of electronics, solar panels, and antennas. Any object at those speeds is a real threat to a satellite. In 2009, Iridium commercial communications satellite and Russian "Kosmos-2251" military satellite collided about 800 kilometres above Siberia in the Low Earth Orbit (LEO). This is the first known example of two satellites colliding in space.10 The commercial communications satellite was destroyed in the collision.

In January 2007, China demonstrated a direct-ascent anti-satellite capability by launching a ballistic missile armed with a kinetic kill vehicle (not an exploding conventional or nuclear warhead) to destroy one of its own aging weather satellites in LEO[11]. The Feng Yun 1-C weather satellite was orbiting at an altitude of about 535 miles above the earth's surface[12]. The deliberate destruction of a satellite by China produced thousands of debris fragments, each of which poses a potentially catastrophic threat to operational spacecraft (Kessler Syndrome)[13]. When initiating a kinetic attack, a country must be willing to forgo

[8] Space Security Index 2007 (2007).
[9] DeBlois, et al (2005).
[10] CelesTrak (2012).
[11] Space Security Index 2007 (2007).
[12] Covault (2007).
[13] Kessler & Cour-Palais (1978).

its own space assets. But the attack can do significant damage to the valuable LEO satellites including most military satellites as well as commercial satellites used for communication. Satellites in the geosynchronous orbit (36,000 km up above the equator) are less vulnerable to anti-satellite missiles.

Other threats, such as space mines, could degrade the performance of all kinds of satellites[14]. One of the most effective threats is a microsatellite in the form of a "space mine." Microsatellite "mines" would collide with other satellites. Even if microsatellites have peaceful and non-weapon military uses – observation, communication, and the like –[15], they make particularly good anti-satellite weapons.

3) Directed-Energy Weapons

A directed-energy weapon uses a beam of electromagnetic energy, either laser light or high-powered radio waves, to destroy a target[16]. For radio waves, the weapon stimulates the target's electronic circuits until they are inoperable. There are two basic laser categories discussed here: low-power lasers and high-power lasers[17]. Low-power lasers are typically designed to spoof or jam satellite electro-optical sensors using laser radiation hence temporarily blinding the satellite. High-power lasers can permanently damage or destroy a satellite by radiating enough energy to overheat its parts. This results in demanding weapon system requirements: high laser power, high beam quality, large aperture beam director, extremely stable beam pointing system, etcetera. These factors make laser weapons extremely complex. Moreover, even if the target's location is known precisely, the laser is useless if smoke or clouds intervene[18].

4) Electronic Jamming Attacks

All military and commercial satellite communications systems are susceptible to uplink and downlink jamming[19]. There are several ways to protect commercial satellite communications systems from potential interferences. These include, for example, data encryption, the use of error protection coding, the employment of directional antennas, and shielding. Further available protection capabilities are currently used primarily for military satellite communications[20].

5) Hijacking

Satellites in the geosynchronous orbit are relay stations suspended 36,000 km above the equator. A communications satellite is simply a radio repeater. Most have 12 or 24 different "transponders" which use a certain frequency block. For Ku band (see Figure 1), the earth station uplink operates in the 14 GHz range. The satellite receives a signal, changes it to the 12 GHz frequency, and sends it back to the earth. Most satellites do not worry about what is modulated on the carrier. They merely translate it and send it back.

[14] DeBlois, et al (2005).
[15] Näsilä, et al (2012).
[16] DeBlois, et al (2005).
[17] GlobalSecurity.org (2012).
[18] DeBlois, et al (2005).
[19] Parry (2012).
[20] Steinberger (2008).

The Tamil Tigers Liberation Front, a Sri Lankan separatist movement, has been blamed for the illegal use of INTELSAT satellites to broadcast radio and TV transmissions via an empty transponder on-board INTELSAT 12 in 2007[21]. INTELSAT 12 is a bent-pipe satellite, which is the most common type of communications satellite mainly because it is much less expensive than the types with an on-board processing. When bent-pipe transponders are not in their full use, the empty transponders can be identified with a spectrum analyzer in combination with a satellite receiver. The empty transponders are configured to re-transmit any signal sent to them. The uplink signal from the hijacker is transmitted to the satellite in a highly-directed beam, which makes the finding of the hijacker extremely difficult[22].

Another satellite interference event occurred in 2002 when the Falun Gong hacked the SinoSat satellite. Interferences in the SinoSat were traced back to a "pirate broadcast operation in Taipei, Taiwan". The interferences disrupted the broadcasts of China Central TV (CCTV) to remote regions of China and the transmissions of China Education TV[23]. During the 2006 Israel-Lebanon war, Israel tried to jam the Al-Manar satellite channel, which is transmitted by the Arab Satellite Communications Organization (ARABSAT), illustrating the potentiality of commercial satellites to become targets during conflicts[24].

Logical Weapons

The supervisory control and data acquisition (SCADA) systems in satellites are designed for and built on old (sometimes decades old) technology and hardware. In addition, their software has been seldom updated. As the SCADA systems become more commonly connected to public and private networks, they are exposed to the standard types of attacks with which many common systems are concerned. In July 2010, a multi-part malware named Stuxnet was discovered. Its main target is the SCADA systems[25]. Stuxnet is primarily disseminated via USB sticks, which allows it to infect computers and networks that are not connected to Internet. Stuxnet is a Trojan horse that specifically looks for a particular model of the Siemens SCADA systems. A rootkit is included in the Trojan to prevent its discovery. If Stuxnet figures that it has found its way into the Siemens systems, it uses a hard-coded password to access the database that the SCADA system uses as a back end. Stuxnet has been found in the SCADA systems in a number of countries, including China, India, Iran and Indonesia. It may have been responsible for the loss of an Indian communications satellite[26]. The satellite's control systems used Siemens S7-400 PLC and SIMATIC WinCC software, both of which are targeted by Stuxnet[27].

Network Attacks

The earth station is connected to an Internet backbone. Unfortunately, Internet connections are susceptible to a variety of attacks, such as spyware, phishing attempts, viruses, backdoors,

[21] Daly (2007).
[22] Daly (2007).
[23] Associated Press (2002).
[24] Space Security Index 2007 (2007).
[25] Woodward (2010).
[26] Woodward (2010).
[27] Woodward (2010).

Trojan horses, and worms[28]. The firewalls in Figure 1 are designed to keep unauthorized outsiders from tampering with the networks of the Finnish Defence Forces. These firewalls include anti-phishing, antivirus and antimalware tools.

The man-in-the-middle is an attack in which an intruder is able to read, insert and modify messages between two parties without either party knowing that the link between them has been compromised. Anyone within satellite coverage can sniff the downloaded data, which normally is unencrypted. A solution to this problem is a virtual private network (see Figure 1). It requires remote network users to be authenticated and secures data with encryption technologies in order to prevent the disclosure of private information to unauthorized parties.

A distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service from the users of the targeted system. A satellite link can be overloaded with pirate broadcasts. Unfortunately, protecting satellite links against the DDoS attacks can be difficult since attackers keep changing their modus operandi.

If the attacker can obtain the Internet Protocol (IP) address of the earth station, it can perform a DDoS attack. The problem with the distributed denial of service attack on Internet is that it is impossible to prevent. This has to do with the distributed nature of the network: every network node is connected with other networks which, in turn, connect to other networks, etcetera. To prevent the DDoS attacks, the earth station should be located in Finland and connected directly to the Finnish Defence Forces intranet.

Welfare Communications and Operational Security Thearts

The welfare communications is an important factor in maintaining morale. Satellites play an important role in the KFOR operation in providing phone, entertainment and e-mail services to operational servicemen (unclassified data, see Figure 1). Everyone from the troops in the field to the highest brass and civilian leaders are allowed to Twitter, blog and use Facebook and other social networking sites29 on the military's unclassified network. The Defence Forces essentially seek to manage the related risks while acknowledging that Internet provides a useful tool for a myriad of tasks. These tasks include, for example, recruitment, public relations, collaboration with a wide range of people and communications between troops and their families.

An Example of Operational Security Threats

If the end-users lack sufficient advice and training on operational security, the utilization of social media poses a serious operational security threat. As noted earlier, obvious operational security threats emerge from the posting of photos on-line and from other visualizations related to the base (see Figure 2), its location, power generators, or communication means.

[28] Steinberger (2008).

[29] Baatarjav & Dantu (2011).

Thus, any information published on-line that relates to an on-going mission, such as, for instance, www.skja.fi (see Figure 2), requires a thorough double-checking in advance.

Figure 2. Photo of a military base from an Internet source[30].

Minimizing Social Media Induced Operational Security Threats

In the protection of soldier identities the usual practice involves introducing each soldier serving in the peace keeping operation only by his or her rank and first name. However, the on-line posting of soldiers' photos with these distinguishing rank and name details compromises operational security since, understandably, an adversary may blackmail soldiers' families in order to, for example, prevent counter-measures against their business activities.

To sum up, the following actions need to be taken into consideration and implemented as a regular part of the standard operating procedure. First, even though on-line connections provide soldiers with a tangible means to increase their overall well-being, issues related to operational security must still be promptly addressed and given the relevance they deserve in the operational hierarchy. Second, all contents posted on-line must be pre-screened either by a security officer or another person authorized to carry out this duty. Third, post-incident reports must remain superficial, and pre-mission information should preferably be classified. Finally, official operation related on-line sites need to be effectively monitored and their contents filtered. This presupposes an artificial intelligence aided program to assist the personnel whose duties include the monitoring of websites. All this contributes to the minimization of the losses that otherwise will inevitably occur due to the human action in network systems. Thus, a man-in-a-loop system as a vigilant and relentless double-checker is necessary in order to enhance operational security and thereby, to facilitate mission success. After all, human beings involved in any operation remain as its weakest links.

[30] SKJA blogi (2012).

Conclusion

The distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby denying the service from the users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down. A satellite link can be overloaded with pirate broadcasts. Unfortunately, protecting satellite links against the DDoS attacks can be difficult since attackers keep changing their modus operandi. In order to prevent the DDoS attacks on the public Internet, the earth station should be located in Finland and be connected directly to the Finnish Defence Forces intranet.

The man-in-the-middle is an attack in which an intruder is able to read, insert and modify the messages between two parties without either party knowing that the link between them has been compromised. Anyone within satellite coverage can sniff the downloaded data which normally is unencrypted. The solution to this problem is a virtual private network, which requires that the remote users of the network are authenticated and data is secured with encryption technologies in order to prevent the disclosure of private information to unauthorized parties.

Welfare communications is an important factor in maintaining morale. Satellite links play an important role in providing phone, entertainment and e-mail services to operational servicemen. In social media the contents of the messages on different platforms (Facebook, Twitter, e-mails, multimedia) cannot be controlled. Thus, a thorough pre-deployment training of troops is a prerequisite for operational security and translates into soldiers not sharing data related to the operation or to the area of operation.

References

Associated Press (2002), “Falun Gong Hijacks Chinese TV,” Available: http://www.wired.com/politics/law/news/2002/09/55350?currentPage=all [May 20, 2012].

Baatarjav, E-A and Dantu, R (2011). “Current and Future Trends in Social Media,” in IEEE Third International Conference on Social Computing (SocialCom) 2011, pp. 1384 – 1385.

CelesTrak (2012). Iridium 33/Cosmos 2251 Collision". CelesTrak. Available: http://celestrak.com/events/collision.asp. [May 20, 2012].

Covault, C (2007). “Chinese Test Anti-Satellite Weapon,” Aviation Week & Space Technology, Jan. 17, 2007.

Daly, J.C.K. (2007, June). LTTE: Technologically innovative rebels. Available: http://www.energypublisher.com/article.asp?id=9803 [May 20, 2012].

DeBlois, Bruce et al. (2005). “Star-Crosses,” IEEE Spectrum, vol. 42, no. 3, March 2005, pp. 40–49.

GlobalSecurity.org (2012). ASATs. Available:
http://www.globalsecurity.org/space/systems/asat.htm [May 20, 2012].

Kessler,D. J. and Cour-Palais, B.G (1978). “Collision Frequency of Artificial Satellites: The Creation of a Debris Belt,” Journal of Geophysical Research, Vol. 83, No. A6, 1978, pp. 2637 - 2646.

Näsilä, A., Saari, H., Antila, J., Mannila, R., Kestilä, A., Praks, J., Salo, H., Hallikainen, M (2012). "Miniature Spectral Imager for the Aalto-1 Nanosatellite", in proc. 4th European CubeSat Symposium, 2012, pp. 24.

Parry, M (2012). “Threats and Vulnerabilities of Government use of Commercial Satcom, SatComs and Navigation“ Available:
http://www2.theiet.org/oncomms/pn/satellite/05%20-%20Mark%20Parry.pdf [May 20, 2012].

Space Security Index 2007. (2007). August, Available: http://www.spacesecurity.org/SSI2007.pdf [May 20, 2012].

Steinberger, J.A (2008). “A Survey of Satellite Communications System Vulnerabilities,” M.S. thesis, Joint Electronic Warfare Center, June 2008.

Vankka, Jouko (2009). “Concept of Finnish Defence Forces SatCom CRO (Crisis Management Operations),” Global MilSatCom 2009 Conference, London, 2009.

Woodward, P (2010). “Israel: smart enough to create Stuxnet and stupid enough to use it. War in Context,“ Available: http://warincontext.org/2010/10/01/israel-smart-enough-to-create-stuxnet-and-stupid-enough-to-use-it/ [May 20, 2012].

SKJA blogi (2012). Available: www.skja.fi [Feb. 29, 2012].

The Care and Maintenance of Cyberweapons

Timo Kiravuo & Mikko Särelä

Abstract

A general with a full arsenal is a happy general. How do you keep your general happy, when any Tuesday a Microsoft update may wipe out most of her military capability?

The analysis of Stuxnet and its cousins shows that the United States (and maybe some other countries) are producing modular cyberweapons software with constant updates, shared components and parallel independent development lines. This article discusses the capabilities needed to create and maintain a cyberweapons arsenal, the components that make up a cyberweapon, and the operative processes for using such weapons.

Keywords: Cyberweapon, Cyberwar, Stuxnet

Introduction

Cyberweapons are software. They do not appear from thin air via virgin birth; someone has to author them. They do not roam freely on the plains of war. Instead, they require computing hardware to process their instructions and thereby, to give them life. These weapons cannot penetrate the target by brute force; they need exposed flaws in the target system.

Cyberweapons would be considered very delicate and fragile things, if they did not have such an impact when they succeed. When the right bit is flipped in the right computer, an entire nation can descend to the blackness of a crashed electric grid. A cyberweapon needs to be up to date on the target system, capable of exploiting a vulnerability which the defenders are not aware of, and able to create the desired impact.

We perceive the cyberweapon only as an instance created from a larger pool of cyber capability. An individual tool has both tactical and operational significance; the toolbox from which these tools are created has strategic significance. Based on what we know about the existing cyberweapons and malware in general, we can describe a likely toolbox structure for future cyber operations and a strategy of constant capability creation to fill up that toolbox.

Architecture

One of the key reasons for the fast development of information society has been the modularity of computer software. A piece of software can perform its task by calling other pieces to do subtasks. As long as the interface of a particular piece is defined, it is easy to join the pieces together. This is in contrast with the mechanical world, where, for example, changing the engine from a car to a different model is generally not trivial – or even possible.

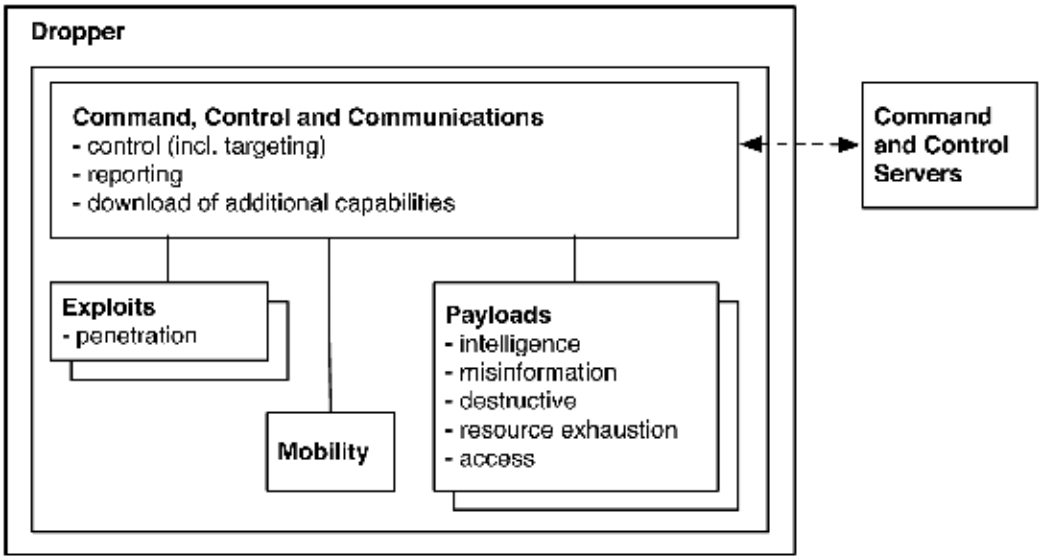


Figure 1: The components and the modular structure of a cyberweapon.

The modular structure in Figure 1 shows how a cyberweapon can be assembled. The components to be deployed to the target system are packaged inside a dropper program which, when activated, installs the weapon into the system. The Command, Control and Communications module directs the operations of the weapon and receives instructions from the Command and Control servers on Internet – if connectivity is available. Exploit modules allow the weapon to access other systems or higher security levels inside the target system, and the mobility module can be used to copy the weapon's code to the newly accessible host. The previous components form the platform assembly of the weapon. This platform carries a payload which is the actual warhead needed to fulfill the mission of the weapon. The mission's requirements decide what modules are assembled to a particular weapon instance.

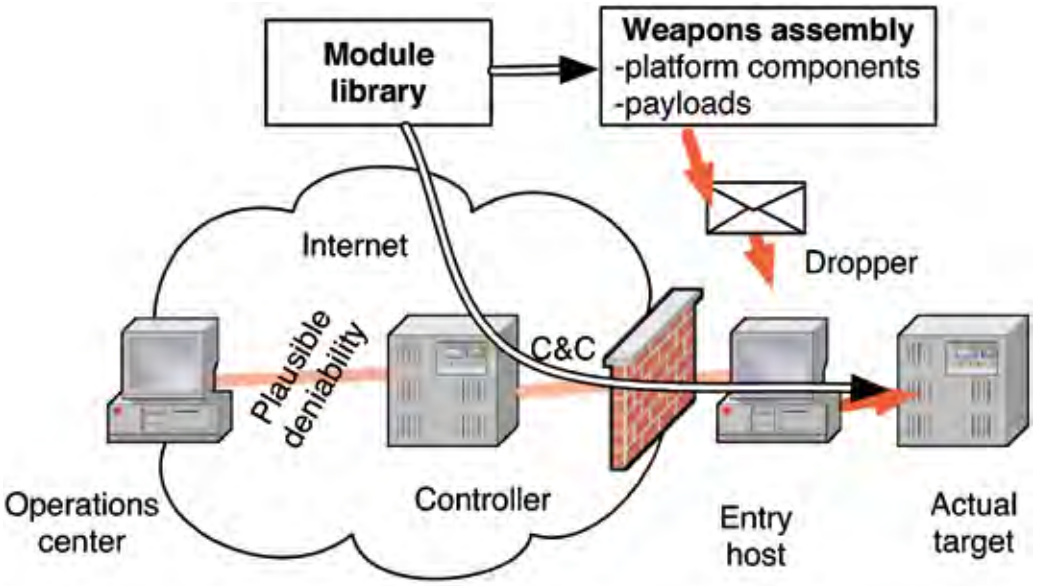


Figure 2: Operations with cyberweapons.

Figure 2 shows how the weapon is assembled from the modules available and deployed by using the dropper, which is packaged in an e-mail message that bypasses the protection of the firewall. Once activated, the weapon connects to its Command and Control servers for instructions and software updates. For example, the payload modules may be kept at the server and be deployed only when needed. This is done to avoid the detection of destructive payloads which, if found, might be used to justify a counterattack.

Payloads

A payload (warhead) is a software program that performs the actual mission of the weapon. The rest of the weapon supports the delivery and execution of this program. Payloads can be classified on the basis of the purpose of the mission. It should be noted that cyberweapons may simultaneously carry and use several payloads.

Intelligence gathering (spyware) payloads can look for files based on the name or the content, analyze the network to which the host machine is connected, use microphone and web camera in the system, collect data from keyboard and display, and so on. This intelligence can then be sent back to the controller of the operation by the available command and control channels. If network connectivity is unavailable, data may be attached to the weapon itself and transported out along with the platform's code by using its mobility capabilities – like a computer virus.

Titan Rain is the US name for a series of organized intelligence gathering attacks against the US computer systems between 2003 and 2005.[1] These attacks were targeted at the defense industry companies and they were persistent, that is, the attackers kept trying to reach the same data by using several different methods.

[1] Mazanec (2009)

The recently observed cyberweapons Duqu and Flame, both of the presumed US origin, have also been used on intelligence gathering missions. Duqu is a Trojan horse (it lacks mobility), which observed payload functionalities include keylogging (keyboard capture), screen capture, and the transmission of selected files from the target host or file shares to the command and control server.[2] Since the payloads are downloaded from the Command and Control servers, the Duqu platform could also be used for other missions.

Flame's payloads have shown similar intelligence gathering features: screenshot and keyboard capture, audio recording, and network traffic snooping. Flame collects especially AutoCAD drawings, e-mails and PDF-documents, and sends them or summaries of them to the control servers.[3]

Misinformation payloads may be used for information warfare. These may take different forms, but are likely to be aimed against specific targets, such as cyber-physical monitoring systems or document stores. Payloads of this type have a huge potential, if they can control the information the opposition leaders see and get inside their OODA loop. Actual operations can be hidden, false operations can be created, logistics misdirected, equipment miscontrolled, and so on.

Thus far, we have not seen cyberweapons that utilize a pure misinformation payload. Stuxnet injected misinformation to the PLC controllers of the refining centrifuges, but the actual goal of Stuxnet was destructive.[4] We believe that misinformation attacks have the potential to distract and misdirect opponents when the cyberweapon is used in combined arms operations.

Destructive (sabotage) payloads may target cyber-physical systems or data. They may delete data from databases and files, or format hard disks. They may also sabotage or destroy physical systems by penetrating the digital systems that control them.

Stuxnet proved the latter case. It was a carefully crafted worm targeted specifically against the Iranian Natanz nuclear enrichment plant.[5] It was designed to be transported inside the plant on a USB thumb drive from which it penetrated the controlling SCADA servers by using known Windows vulnerabilities. After the penetration, the code ran on the server and programmed the controllers of the enrichment centrifuges to change their speed, which caused the high-speed centrifuges to break.

Stuxnet was created by the United States and Israel[6] and it served two political goals: to slow down the Iranian nuclear weapons program and to avoid the use of conventional military force in this attempt. While the details of the Stuxnet program are not public, it has been estimated that the project might have been realized with only a couple of dozens of programmers and analysts and a budget in the order of millions of dollars.[7] Before the administration of the United States decided to reveal its involvement, Stuxnet also provided plausible deniability – unlike a kinetic attack would have done.

[2] Gostev et al. (2011); Bencsáth et al. (2012); Bencsáth et al. (2012)
[3] sKyWIper Analysis Team (2012); Gostev (2012b)
[4] Sanger (2012)
[5] Falliere et al. (2010)
[6] Sanger (2012)
[7] Gostev et al. (2011)

Resource exhaustion payloads can be used to deny a resource temporarily or to distract its defenders. These attacks usually rely on brute force and can, for example, shut down a web server by sending requests constantly from thousands of hosts or a network link by flooding it with traffic (called Distributed Denial of Service or DDoS). The hosts are often acquired by inflicting consumer computers with malware and thereby, gaining control of a large amount of computers (called "botnet") in different network locations. Resources can be overloaded by data or simple queries, but also with complex requests that generate severe processing at the target system.

When a Soviet era statue was moved in Tallinn in 2007, cyber attacks were targeted against Estonian web sites. These "Bronze Soldier" attacks shut down the web servers for a few days. Similar attacks took place during the South Ossetian war in 2008.[8] These kinds of DDoS attacks have mostly propaganda and nuisance value, if they are targeting non-essential government web servers. When a web server is overloaded, it will return to normal use once the attack stops. Nonetheless, resource exhaustion attacks have potential for blocking critical cyber-physical controllers, logistics systems, servers for retail payment systems, and so on.

Access payloads have the goal of breaking into a system and allowing their operators to gain online access. Firewalls typically consider the internal network trustworthy and thus, allow the opening of connections from inside to outside. Experiments have shown that, for example, by seeding a parking lot with USB memory sticks, a company's computers can be infected with software that connects back to its control server.[9]

The access may be used by human operators or by computer software. The US defense research organization, DARPA, is currently researching automated mission scripts that perform actions under human supervision, but at computer speed.[10]

The Platform

The payload needs a supporting platform that delivers it to the right place and provides it with command and control. To create a weapon, the platform needs several types of modules that are integrated with each other and the payload.

For a force to be considered "cyber capable" these components must exist before a need arises, so that the weapon can be put together for a mission within a reasonable timeframe.

Command, Control and Communications Module

A cyberweapon may operate autonomously or it can be remotely controlled. An autonomous weapon must have its own logic programmed to control its payload activities and mobility, including the decision of whether to trigger the payload or not. For example, Stuxnet was designed to evaluate its surroundings and to deploy the payload only if it was in the right environment.

[8] Deibert et al. (2012)
[9] Stasiukonis (2006)
[10] DARPA (2012)

Having a control channel back to a command and control server (C&C) allows the weapon to upload its findings, as well as to receive instructions and new capabilities (software modules) back. A C&C channel increases the potential for detection, but it has several benefits over autonomous operations. Parts of the operational logic can be kept at the server, so that if the weapon is detected, its purpose may remain hidden. In addition, the channel may be used to keep a human being in the loop to guard against accidental releases of payload effects.

The C&C channel can be a connection to a web server or to an e-mail server and thus, appear to firewalls and intrusion detection systems as routine traffic. Internet Relay Chat (IRC) can be used to control multiple hosts, such as botnets, because it is better suited for sending real time messages to multiple recipients. Other common methods include the use of DNS name services or protocols that are used by video games. The point is to hide the communications among other data. If the weapon is found and dissected, the addresses used for communications will be found and analyzed.

Another function of the command and control channel is to provide separation between the weapon and its operators. A properly constructed command and control system includes a sufficient number of cutouts (connections that cannot be traced back, for instance, using public WLAN in a popular place) to hide the identity of the owner of the weapon. This creates deniability, which is useful for keeping cyber operations from escalating to kinetic war. Stuxnet achieved this: it performed a strike without leaving the opponent a casus belli for lawful retaliation – until the US administration revealed its involvement.11

Vulnerabilities and Exploits

A cyber weapon needs a delivery system that can guide the payload into the target. This is where software vulnerabilities and matching methods (exploits) to abuse them come into play.

Vulnerabilities are created into software during the programming process and they can be considered emergent features due to the complexity of the software environment. These programming mistakes are unavoidable with the current practices and architectures. Typically, data received from the network is passed around within the various parts of the software. At some point the data is processed by a piece of code that was written by a programmer who did not realize that the input could be malicious. For example, a line of text might be longer than the specification allows and thus writes over some memory areas. These vulnerabilities have been found by analyzing the binary or the source code of the software in most operating systems, network server programs and programs accessible only from the inside. It is possible that future programming practices and software architectures lessen the amount of vulnerabilities in software.

According to some recent reports, the price of a new, unpublished vulnerability (so called zero-day vulnerability) for popular operating systems is in the order of hundreds of thousands of

[11] Sanger (2012)

dollars.[12] Defense manufacturers, such as Vupen[13], are already purchasing and selling these.[14] This creates incentives for programmers to intentionally create vulnerabilities – secretly from their employers – so that they can later cash the rewards from defense manufacturers.

Not all attacks need network vulnerabilities to gain access to a system; cyberweapons may also be sent over e-mail (Duqu), on USB sticks (Stuxnet), or they can be acquired and installed by the target from web sites. If the user or the operating system at the target system allows executing the software, network based security can be bypassed.

Droppers

To deliver the weapon to the target system, a separate dropper component can be used as a platform carrier. The dropper packs the rest of the software into an e-mail message, a web page, a software update, an auto-executable file on a USB drive, or into some other initial delivery vector. When activated, the dropper installs the weapon code to the target system and activates it. The code may masquerade as a device driver or a software update, and it may be signed cryptographically in such a way that the target operating system will accept it as a valid update. Current software certification systems are known to be lacking, which makes it possible to acquire or manufacture false credentials. Stuxnet and Duqu use installation files signed with stolen certificates in order to appear legitimate; Flame manages to sign itself with a Microsoft certificate when spreading.[15]

The actual software code can be included in the same package as the dropper, or it can be downloaded from Internet by the dropper. The dropper program can contain its own stealth methods, for example, the Duqu dropper waits for a ten minute period of no keyboard activity before it initiates its operations.

To give an example, one of the methods used to inject the commercial FinFisher[16] surveillance product to the target workstation is to send an e-mail message with the program included. To avoid alerting the recipient that the attachment is an executable program, it is named "gjp.1bajaR.exe" with the Unicode "right-to-left override" character as the first character. This causes the file name to appear as "exe.Rajab1.jpg".[17]

Mobility Module

If the system to be penetrated is protected by a firewall, an air gap (no direct network connectivity) or some other method preventing a direct access from the command and control servers, a self-replicating mobile code may be used. This, in effect, turns the weapon into a worm or virus. Viral mobility of the weapon makes it more likely to be detected and thus, leaving the mobility out can be reasonable. This, in effect, reduces the weapon to a Trojan horse that targets only a single system.

[12] McKinney (2007)
[13] http://www.vupen.com
[14] Schneier (2012)
[15] Gostev (2012c)
[16] http://www.finfisher.com
[17] Marquis-Boire (2012)

Stuxnet used known Windows vulnerabilities in printing and server systems to gain access to critical servers and, as the network was supposed to be inaccessible from the outside, the systems had not been updated to the latest security level.[18] Stuxnet also used network file shares to spread and a hardcoded password to enter Siemens' WinCC SCADA server.[19] Flame, again, uses several methods for spreading to new hosts – one of which is masquerading as a Microsoft Windows Update server. This feature allows it to send itself to the target machine as a Windows Gadget update. [20]

Features

In addition to the prepared modules, there are several features that are useful for a cyberweapon. These do not form their own modules, but have to be implemented in modules, architecture and during integration.

Stealth

In general, low probability of detection is a desirable feature in cyberweapons (unless distraction is required). This is not a property of any individual component, but a property that emerges from the overall design and operation of the weapon. Detection can be avoided with such features as slow propagation rate, small size, ability to hide in the operating system, and low activity level when human operators are present. A common way to hide in the operating system for both intruders and malware is to masquerade as utility programs, device drivers, software libraries and such, and to modify or replace the analysis tools with versions that do not show the processes and files of the malware or the intruder. Stealth during the installation may be assisted by acquiring valid installation certificates for the cyberweapon.

To avoid detection and analysis, a cyberweapon may remove its tracks in various ways. A sensible guideline would be to remove any component, like the dropper, when it is no longer needed. If possible, the weapon should analyze the backup service in the target system and to try to avoid an inclusion into the backup.

For example, Duqu waits for a ten minute period of user inactivity before it starts to install itself to the operating system. After 30 days Duqu uninstalls itself – unless it has been instructed to remain.[21]

Hidden Components

To avoid analysis, parts of the weapon can be encrypted without including the decryption key in the software itself. The key to activate the encrypted portion may be transmitted from

[18] Falliere et al. (2010)
[19] Falliere et al. (2010)
[20] Gostev (2012c)
[21] Symantec (2011)

an operations center or it may be created (via a cryptographic hash) from the environmental parameters the weapon will encounter only when it reaches the target system.

The Gauss malware, related to Flame, carries a payload that is encrypted with a key derived from the environment variables in the target system. Thus, it triggers the warhead when the weapon hits a system with the correct variables.[22] Contents of the payload are unknown at the time of writing.

Countermeasures after Detection

To avoid analysis and to gain time, future cyberweapons may include functionality to defend themselves from detection. There is no trivial way to identify detection, but access to the weapon's files or processes may indicate an attempt to detect it – as does the use of its system tools. If the weapon estimates that it has been detected or that the detection is likely, it can activate countermeasures, such as spreading rapidly virally, mutating itself to avoid analysis, or even spawning a hidden copy of itself or of a different weapon. The goal is not so much to avoid detection as to gain time by increasing the defender's workload. Human detection and analysis move at human speed, while software moves in a sub-second time frame. Depending on the mission, the weapon might gain mission success even after an initial detection by avoiding analysis and keeping the defenders occupied.

Kill Switch

For various reasons it may be desirable that the operation of a cyberweapon is halted. For weapons that are able to connect to Internet, this may be a message from the control server. To protect the weapon, this message may be cryptographically signed to verify its authenticity (using asymmetric encryption means that the detection of the decryption key does not enable anyone to send the kill message). Another method to kill the weapon would be to prepare an identification string and the removal instructions for anti-viral software. These instructions ought to be published if needed.

Claiming Credit

If the owner of a cyberweapon wishes to claim credit for it, for example, in order to use a particular operation for deterrence, the weapon may contain cryptographically signed or encrypted data. The owner can then prove the ownership of data by revealing the key.

Operational Integration

As discussed earlier in this article, a modular architecture is a likely solution to be employed in the creation of a cyberweapons capability in the long run. Modularity allows the actual weapons to be crafted according to the operational requirements, which increases flexibility and decreases costs. However, modularity is not without its own issues.

[22] Global Research & Analysis Team (2012b)

For a modular system to work, the interfaces between the components and the architecture need to be well defined. Ideally, it should be possible to create a weapon by just selecting its desired functionality and assembling the components. However, this might produce fairly recognizable weapons. During the integration process the names of the files (cyberweapons may masquerade as systems libraries or device drivers) can be changed, the structure modified, and so on. This is done to give the weapon a form that is not easily detectable.

To make the detection harder, a compiler can be modified to randomize the structure of the code. This makes each instance of the weapon unique and hence more difficult to recognize by antiviral software and other tools. There could be several libraries that are randomly used to implement the same higher layer primitives. Alternatively, different machine language operands can be used for the same low level function. In a similar way, dropper programs may be created in a way that makes them appear unique. Each target system could then be targeted with an individual binary.

Integration testing is generally considered useful. However, thorough testing takes time that may not be available. It can be assumed that any cyberweapon will have defects, and that some of these defects will cause unintended consequences. For example, an autonomous cyberweapon may start to spread more rapidly and widely than intended, or it may target wrong systems, including the operator's own systems. It may also simply fail to work.

Organizing the Cyber Capability

Offensive cyber capability requires a continuous process of collecting vulnerabilities, creating exploits, platforms and warheads, and building a network of deniable hosts on Internet to maintain the secrecy of the operator. As these are low cost operations (in comparison to kinetic military capabilities), it can be argued that these preparations should be made even if the current doctrine does not include the use of offensive cyber capabilities.

Organizing the Development Process

It has been estimated that Stuxnet was built by a team of perhaps 20 to 30 people.[23] On the basis of what is known about software engineering in general, this appears likely. The sensible way to produce the modules for cyberweapons is to have small focused teams working on different module lines and supporting functions, such as integration and testing.

One of the benefits of cyberweapons is their plausible deniability. All operations should be run with the assumption that any deployed weapon will be found, analyzed and reverse-engineered. For this reason, the teams should use different styles and tools. Modules deployed in the weapons should be grouped in such a way that the connection of a weapon with its creators does not reveal all deployed weapons.

Stuxnet (discovered in 2010) can be considered the first observed cyberweapon (this depends on the viewpoint). When Duqu was discovered in 2011, it was found to use the

[23] Gostev et al. (2011)

same platform. Thus, it was believed to have been developed by the same organization – just employing a different payload.[24] In 2012, when Flame was discovered, it was also assumed to be part of the US cyber operations in the Middle East, but initially no direct link was found to Stuxnet (that had been revealed to be a US operation). However, analysis suggests that Flame and Stuxnet have also been produced by the same organization.[25] When Gauss was found later in 2012, it was soon linked to Flame. This tied all of these cyber weapons together by various components.[26]

Altogether, this shows that the US cyber operations have several "product lines" using shared components to produce cyberweapons for different missions. From the estimate of the size of the Stuxnet team, it can be extrapolated that the operation might have a staff of between 50 and100 programmers and computer specialists. This estimate does not include the intelligence operatives who are the actual customers of the weapons. This organization allows a rapid creation of cyber weapons for different purposes. However, as shown, it has not provided deniability since the weapons have been linked to each other.

Command and Control Servers

Cyber attacks may be controlled from the attacker's own computers (leading to easy detection) or, more preferably, from deniable computers that are either captured third party computers or legally acquired hosts. A suitable controller would be a server host from a cloud server which can be easily acquired and at a low cost. Any competent intelligence organization should be able to organize a process for acquiring a set of untraceable servers spread to different places internationally.

Conclusion

A long term strategic process for integrating the cyber-dimension to existing military capabilities can be described as follows. Learn the capabilities of cyber weapons. Create a cyber-command leadership that understands these capabilities. Communicate these capabilities to other branches in the military and intelligence community. Make sure that enough knowledge is available for military operations planning. Knowledge of cyber capabilities should be available to the planners so that cyber operations can be used to support or replace conventional operations.

Cyber capability should be viewed as the light cavalry. It is a force for reconnaissance, distracting the enemy, probing attacks and dedicated operations behind the lines. Cyber capabilities provide support in combined arms attacks and can, occasionally, be used for selective strikes. Software does not hold ground.

[24] Gostev and Soumenkov (2011)
[25] Gostev (2012a)
[26] Global Research & Analysis Team (2012a)

References

We apologize for the large amount on online sources that have not been peer-reviewed. In our belief these analyses reflect the best currently available information on cyberweapons.

Symantec (2011 W32.Duqu: The precursor to the next Stuxnet. Symantec. Online: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf Retrieved Sep 20, 2012.

DARPA (2012). Plan X proposers' day workshop. Defense Advanced Research Projects Agency. Online: https://www.fbo.gov/index? s=opportunity&mode=form&id=19cced1c188775a844f889872c64c30f Retrieved Oct 23, 2012.

Bencsáth, B., Pék, G., Buttyán, L., and Félegyházi, M. (2012). Duqu: Analysis, detection, and lessons learned. *Proceedings of 2012 European Workshop on System Security*.

Deibert, R. J., Rohozinski, R., and Crete-Nishihata, M. (2012). Cyclones in cyberspace: Information shaping and denial in the 2008 RussiaGeorgia war. *Security Dialogue*, 43(1).

Falliere, N., Murchu, L., and Chien, E. (2010) W32.Stuxnet dossier. Online: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf Retrieved Oct 24, 2011.

Global Research & Analysis Team, K. L. (2012a). Gauss: Nation-state cyber-surveillance meets banking Trojan. Online: http://www.securelist.com/en/blog/208193767/Gauss_Nation_state_cyber_surveillance_meets_banking_Trojan Retrieved Nov 1, 2012.

Global Research & Analysis Team, K. L. (2012b). The mystery of the encrypted Gauss payload. Online: http://www.securelist.com/en/blog/208193781/The_Mystery_of_the_Encrypted_Gauss_Payload Retrieved Nov 1, 2012.

Gostev, A. (2012a). Back to Stuxnet: the missing link. Online: https://www.securelist.com/en/blog/208193568/Back_to_Stuxnet_the_missing_link Retrieved Nov 2, 2012.

Gostev, A. (2012b). The Flame: Questions and answers. Online: http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers Retrieved Aug 30, 2012.

Gostev, A. (2012c). 'Gadget' in the middle: Flame malware spreading vector identified. Online: http://www.securelist.com/en/blog/208193558/Gadget_in_the_middle_Flame_malware_spreading_vector_identified Retrieved Sep 20, 2012.

Gostev, A. and Soumenkov, I. (2011). Stuxnet/Duqu: The evolution of drivers. Online: http://www.securelist.com/en/analysis/204792208/Stuxnet_Duqu_The_Evolution_of_Drivers Retrieved Nov 2, 2012.

Gostev, A., Soumenkov, I., and Kamluk, V. (2011). The mystery of Duqu: Parts 1-10. Online: http://www.securelist.com/en/blog/208193182/The_Mystery_of_Duqu_Part_One Retrieved Sep 20, 2012.

Marquis-Boire, M. (2012). From Bahrain with love: FinFisher's spy kit exposed? Online: https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/ Retrieved Sep 23, 2012.

Mazanec, B. (2009). The art of (cyber) war. *Journal of International Security Affairs*, (16):84. McKinney, 2007] McKinney, D. (2007). Vulnerability bazaar. *Security Privacy, IEEE*, 5(6):69 –73.

Sanger, D. E. (2012). Obama order sped up wave of cyberattacks against Iran. *New York Times June 1 2012*.

Schneier, B. (2012). The vulnerabilities market and the future of security. *Forbes Sep 21, 2012.*

sKyWIper Analysis Team (2012). sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks, v1.05. Online: http://www.crysys.hu/skywiper/skywiper.pdf Retrieved Sep 20, 2012.

Stasiukonis, S. (2006). Social engineering, the USB way. Online: http://www.darkreading.com/security/article/208803634/index.html Retrieved Jan 17, 2011.

The Exploit Marketplace

Mikko Hyppönen

Abstract

Weaponized exploit code to attack vulnerabilities in operating systems and applications have become the everyday trading goods of the cyber armament industry. Several boutique companies specializing in finding zero-day vulnerabilities have popped up in various countries. These companies go out of their way to find bugs that can be exploited and turned into security holes. Once being found the bugs are weaponized. In this way, they can be abused effectively and reliably. These companies also make sure that the home company of the targeted product will never learn about the vulnerability - because if it did, it would fix the bug. Consequently, the customers and the public at large would not be vulnerable anymore. This would make the exploit code worthless to the vendor. It is surely a weird business to be in.

Keywords: Cyber, code, vulnerabilities, exploits, marketplace.

I used to like Western movies. I loved John Wayne, Marlon Brando and Clint Eastwood. There was something deeply comforting in the simplified storylines of good guys and bad guys: the bad guys in their black cowboy hats wanting to steal and kill and the good guys with white hats coming and stopping them from doing that.

Unfortunately, in the real world things are not that black and white. This is especially true in the world of cybercrime and online attacks. There are various players behind such attacks, with completely different motives and with different techniques. If one wants to defend against these attacks effectively, one has to be able to estimate who is most likely to attack and why.

The attackers include organized criminals gangs (who are after money); hactivists movements, like the Anonymous (who do it for a protest or for a political motive); and governments (who do it for espionage or to affect their enemies indirectly).

The Need for Exploits

Even if the aforementioned groups have nothing to do with each other, they have one thing in common: they all need exploits. They need them for gaining access to systems they should not be on.

There is no exploit without a vulnerability. Ultimately, vulnerabilities are just bugs, that is, programming errors. We have bugs because programs are written by people, and people make mistakes. Software bugs have been a problem for as longs as we have had programmable computers – and they are not going to disappear.

Bugs were not very critical until Internet became widespread. You could have been working on a word processor and opening a corrupted document file, and, as a result, your word processor would have crashed. Even if annoying, such a crash would not have been too big of a deal. You might have lost any unsaved work in open documents, but that would have been it. However, things changed as soon as Internet entered the picture. Suddenly, bugs that used to be just a nuisance could be utilized to take over one's computer.

Different Vulnerabilities

Contemporarily, we have different classes of vulnerabilities and their severity ranges from a nuisance to a critical vulnerability.

First, we have local and remote vulnerabilities. Local vulnerabilities can only be exploited by a local user who already has access to the system. At the most extreme, certain hardware-based vulnerabilities can only be exploited by a user who can physically access the machine (for example, vulnerabilities based on gaining physical access to the USB, HDMI or Firewire port of the device). Remote vulnerabilities are much more severe as they can be exploited from anywhere over a network connection.

Vulnerability types can then be divided according to their actions on the target system: Denial of Service, Privilege Escalation or Code Execution. Denial of Service vulnerabilities allow the attacker to slow down or shut down the system. Privilege Escalations can be used to gain additional rights on the system, and Code Execution allows running commands.

The most serious vulnerabilities are Remote Code Execution vulnerabilities. These are what the attackers need.

Yet, even the most valuable vulnerabilities are worthless, if they get patched. Therefore, the most valuable exploits are targeting vulnerabilities that are not known to the vendor behind the exploited product. This means that the vendor cannot fix the bug and issue a security patch to close the hole. If a security patch is available and the vulnerability starts to get exploited by the attackers five days after the patch came out, the users have had five days to react. If there is no patch available, the users have no time at all to secure themselves; literally, zero days. This is where the term 'Zero Day Vulnerability' comes from: users are vulnerable, even if they have applied all possible patches.

The knowledge of the vulnerabilities needed to create these exploits is gathered from several sources. Experienced professionals search for vulnerabilities systematically by using techniques like fuzzing or by reviewing the source code of open source applications and looking for bugs. Specialist tools have been created to locate the vulnerable code from compiled binaries. Less experienced attackers can find known vulnerabilities by reading security themed mailing lists or by reverse engineering security patches as they are made available by the affected vendors. Exploits are valuable even if a patch is available, because there are targets that do not patch as quickly as they should.

Originally, only hobbyist malware writers were using exploits to do offensive attacks. Worms, like Code Red, Sasser and Blaster, would spread around the world in minutes as they could remotely infect their targets with exploits.

Things Changed

Things changed when organized criminal gangs began making serious money with keyloggers, banking trojans and ransom trojans. When money entered the picture, the need for fresh exploits created an underground marketplace.

Things changed even more when the governments entered the picture. When the infamous Stuxnet malware was discovered in July 2010, security companies were amazed to notice that this unique piece of malware was using a total of four different zero-day exploits – which remains a record in its own field. Stuxnet was eventually linked to the Operation Olympic Games – an intelligence and military operation launched by the governments of the United States and Israel to target various targets in the Middle East and, especially, to slow down the nuclear program of the Islamic Republic of Iran.

Other governments learned from the Operation Olympic and saw its three main takeaways: attacks like these are effective, they are cheap, and they are deniable. All of these qualities are highly sought after in espionage and in military attacks. In effect, this started a cyber arms race which today is reality in most of the technically advanced nations. These nations were not just interested in running cyber defense programs to protect themselves against cyber attacks. They wanted to gain access to offensive capability and to be capable of launching offensive attacks.

Offensive Cyber Programs Looking for New Exploits

Exploits do not last forever. They get found out and patched. New versions of the vulnerable software may require new exploits, and these exploits have to be weaponized and reliable. To have a credible offensive cyber program, a country needs a steady supply of fresh exploits.

As finding the vulnerabilities and creating weaponized exploits is hard, most governments would need to outsource this job to experts. Where can they find such expertise from? Security companies and antivirus experts are not providing attack codes; they specialize in defense, not in attacking. Intelligence agencies and militaries have always turned to defense contractors when they have needed technology which they cannot produce by themselves. This applies to exploits as well.

By simply browsing the websites of the largest defense contractors in the world, one can easily find out that most of them advertise offensive capabilities to their customers. Northrop Grumman even runs radio ads claiming that they "provide governmental customers with both offensive and defensive solutions".

However, even the defense contractors might have a hard time building the specialized expertise to locate unknown vulnerabilities and to create attacks against them. Many of them seem to end up buying their exploits from one of the several boutique companies that specialize in finding zero-day vulnerabilities. Such companies have popped up in various countries. These companies go out of their way to find bugs that can be exploited and turned into security holes. Once being found the exploits are weaponized. In this way, they can be abused effectively and reliably. These attackers also try to make sure that the company behind the targeted product will never learn about the vulnerability – because if it did, it would fix the bug. Consequently, the customers and the public at large would not be vulnerable anymore. This would make the exploit code worthless to the vendor.

Companies specializing in selling exploits operate around the world. Some of the known companies reside in the United States, in the UK, Germany, Italy and France. Others operate from Asia. Many of them like to portray themselves as part of the computer security industry. However, we must not mistake them for security companies, as these companies do not want to improve computer security. Quite the opposite, these companies go to great lengths to make sure that the vulnerabilities they find do not get closed – and by doing this, they make us all more vulnerable.

In some cases, exploits can be used for good. For example, the sanctioned penetration tests done with tools such as Metasploit can improve the security of an organization. However, that is not what we are discussing here. Instead, we are talking about the creation of zero-day vulnerabilities to be used only for offensive attacks.

The total size of the exploit export industry is hard to estimate. However, by looking at the public recruitment ads of the known actors as well as of various defense contractors, it is easy to notice that there is much more recruitment taking place right now for offensive positions than for defensive roles. As an example, some US-based defense contractors have more than a hundred open vacancies for people with TOP SECRET/SCI clearance to create exploits. Some of these vacancy ads specifically mention the need to create offensive exploits targeting iPhones, iPads and Android devices.

If we look for offensive cyber attacks that have been linked back to a known government, the best known examples link back to the governments of the United States and Israel. When The New York Times ran the story which linked the US Government and the Obama administration to the Operation Olympic Games, the White House started an investigation on who had leaked the information. Note that they never denied the story. They just wanted to know who leaked it.

Exploits Blur the Lines between Black and White Hats

As the United States is conducting offensive cyber attacks against other countries, other countries certainly feel that they are free to do the same. This cyber arms race has created an increasing demand for exploits. The resulting exploit industry is further blurring the lines between the black hats and the white hats.

I used to like Western Movies. Sadly, I think time for them is now well behind us.

The Fog of Cyber Defence is a book about cyberspace, cyber security and cyberwar. The book is untangling the ties of the Nordic states with the important, yet complex and foggy phenomenon of cyber. It is adding important perspectives into the ongoing discussion about cyber security and creating room for the deepening of co-operation amongst the Nordic states. The articles in the book contribute to the debate over the implications of cyber for national security and the armed forces. The authors, who come from various professional backgrounds, appreciate and welcome further discussion and comments on the very important themes that impact our everyday lives.

Editors

Jari Rantapelkonen

Mirva Salminen

Authors

Sakari Ahvenainen
Kari Alenius
Jan Hanska
Roland Heickerö
Simo Huopio
Mikko Hyppönen
Margarita Jaitner
Saara Jantunen
Harry Kantola
Timo Kiravuo
Erka Koivunen
Anssi Kärkkäinen
Jarno Limnéll
Kristin Mørkestøl
Rain Ottis
Tero Palokangas
Jari Rantapelkonen
Tapio Saarelainen
Mikko Särelä
Topi Tuukkanen
Jouko Vankka

National Defence University
Department of Leadership and Military Pedagogy
P.O. Box 7, 00861 Helsinki
Suomi • Finland

Tel: +358 0299 800
www.mpkk.fi

ISBN: 978-951-25-2430-3
ISBN: 978-951-25-2431-0 (PDF)
ISSN: 1798-0402