An Evaluation of State-Level Strategies Against Botnets in the Context of Cyber Conflicts

Christian Günter Czosseck

Doctoral Thesis in Management | No. 14 | Tallinn 2012

Estonian Business School

Estonian Business School

AN EVALUATION OF STATE-LEVEL STRATEGIES AGAINST BOTNETS IN THE CONTEXT OF CYBER CONFLICTS

Dissertation for a Doctor of Philosophy Degree
by
Christian Günter Czosseck

Tallinn 2012

Department of Information Technology, Estonian Business School, Estonia

Dissertation is accepted for the defence of the degree of Doctor of Philosophy in Management by the Research council of the Estonian Business School on July 18, 2012.

Supervisor: Professor Peeter Lorents, Ph.D.
Chair of the Department of Information Technology
Estonian Business School, Estonia

Opponents: Gabriel Jakobson, Ph.D.
Chief Scientist
Altusys Corporation
Princeton, USA

Professor emeritus Leo Võhandu, Ph.D.
Tallinn University of Technology
Tallinn, Estonia

Public Commencement on November 19, 2012 at Estonian Business School, Lauteri 3, Tallinn.

ISBN 978-9949-9292-6-9 (print)
ISBN 978-9949-9292-7-6 (PDF)

EBS Print, Lauteri 3, Tallinn

ACKNOWLEDGEMENTS

I am profusely thankful to my supervisor, Professor Peeter Lorents, for all his continuous encouragement as well as dedicated guidance and support on my way to completing this dissertation.

Furthermore, I want to thank all those people I have met in the past years and who supported me by sharing their experience and wisdom.

While there are many more, I would like to especially thank Dr. Robert J. Pefferly and Dr. Rain Ottis and Mr. Karlis Podins, who over many discussions helped me to find my way.

Further, I want to express my appreciation to my opponents, Dr. Gabriel Jakobson and Dr. Leo Võhandu, as well as all the anonymous peer reviewers of my publications for their constructive comments and suggestions.

Finally, I want to express my greatest gratitude to my wife Carmen Czosseck, who supported me through all the years of working on my dissertation and gave me the backup I needed for finishing this research.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Botnets, global networks of infected computers under the central control of its botnet master, have been around for decades, primarily as a means for cyber criminals to obtain money illegally. While having been a nuisance in the past, botnets now pose a serious threat to the economies of most internet-dependent countries.

The cyber attacks against Estonia back in 2007 can be seen as a turning point in the attention States pay towards the question of cyber security. This is reflected in the dramatic increase of new or revised national cyber strategies, recognizing that threats originating from cyberspace represent a new form of threat to national security.

While the impact on Estonia was not as severe as commonly believed, it highlighted the increasing threat of politically motivated cyber attacks conducted by groups of people, as well as new ways nations are using cyberspace and such groups for their benefit. Botnets are one weapon of choice for such attacks.

The research presented in this dissertation focuses on the changing role of botnets as a major part of the new landscape of threats in the 21st century for private and public sectors alike, but from different standpoints.

The research conducted here uses theoretical and empirical research methods to firstly explore the changing role of botnets in cyber conflict in general in order to support IT security managers, cyber security experts or policy advisers, especially in governments. It presents a definition and identifies the unique features of cyber weapons and consequently develops a way of looking at cyber conflict by focusing on the role of knowledge about vulnerabilities in IT systems.

A taxonomy of botnet usage in cyber conflict is presented and the research further analyses the resources needed for a takedown of a botnet from an organizational perspective.

The dissertation then develops a comprehensive framework of State-level botnet mitigation strategies. Using the established DEMATEL method and knowledge empirically gathered from experts in different domains, this set of strategies is evaluated in respect to its impact on the threat posed by botnets. As a result, the research offers a justified ranking and recommendation for these strategies to those concerned with national cyber security.

Keywords: cyber security, cyber attack, cyber weapon, strategy evaluation, DEMATEL method, botnets, taxonomy

LIST OF PUBLICATIONS

The contribution of this thesis is based on the following academic publications and referred to hereinafter using the following titles in bold.

Publication I

Czosseck, C. and Podins, K. 2012. A Vulnerability-Based Model of Cyber Weapons and its Implications for Cyber Conflict. In *Proceedings of the 11th European Conference on Information Warfare and Security*. Laval: Academic Publishing Limited, 198-205.

Publication II

Czosseck, C. and Podins, K. 2011. An Usage-Centric Botnet Taxonomy. In *Proceedings of the 10th European Conference on Information Warfare and Security*. Tallinn: Academic Publishing Limited, 65-72.

Publication III

Czosseck, C., Klein, G. and Leder, F. 2011. On the Arms Race Around Botnets - Setting Up And Taking Down Botnets. In *Proceedings of the 3rd International Conference on Cyber Conflicts*. Tallinn: CCD COE Publications, 107-120.

Publication IV

Czosseck, C., Ottis, R., Talihärm, A.-M. 2011. Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security. In *Journal of Cyber Warfare and Terrorism*, 1 (1), 24-34.

Publication V

Czosseck, C. 2012. Evaluation of Nation-state Level Botnet Mitigation Strategies Using DEMATEL. In *Proceedings of the 11th European Conference on Information Warfare and Security*. Laval: Academic Publishing Limited, 94-103.

INTRODUCTION

The Threat Posed by Botnets

The term *botnet* refers to the use of malware (often but not always advanced malware) to obtain unauthorized and ideally undetected on-going access to a large number of victim computer systems. An essential function of this malware is the capability to connect back to a Command and Control (C&C) infrastructure built by the creator of the botnet to execute remote control over the infected computer systems referred to as bots[1] or zombies. This ultimately forms a network of bots, a botnet, putting its creator into a position where he can conduct malicious activities on a large scale (Plohmann, Gerhards-Padilla and Leder 2011; Kola 2008; OECD 2008).

Nowadays, botnets are the main instrument among others used for organized cyber crime such as executing spam campaigns, threatening companies via DDoS[2] attacks to pay fees to criminals or extorting money by planting ransom ware on the infected systems. They are also frequently used to steal sensitive data[3] from companies and individuals[4] (Kola 2008; OECD 2008).

While having been a nuisance in the past, most high-tech economies that depend on free access to the internet among other things, are facing a serious threat. For example, the UK economy alone is said to suffer from 27 bn GBP in damages and losses per year from cyber crime (UK Cabinet Office and Detica Ltd. 2011). Others estimate the damage done to individuals globally to 388 bn USD annually (Symantec 2011).

Besides earning money illicitly being the major driver behind this development, cyber attacks by individuals or groups for political reasons has emerged as a new type of threat. This threat is commonly referred to as hacktivism[5] (Denning 2001a; Ottis 2010). Hacktivists select their targets differently and often target highly visible victims primarily in the private sector (Czosseck, Ottis and Talihärm 2011).

The cyber attacks against Estonia serve as one of many examples from the recent past. In April 2007, over the course of 22 days, the Government of Estonia and

---

[1] short for robot

[2] Distributed Denial of Service, short DDoS, is a cyber attack there a large number of computer systems is issuing requests to a single target system (e.g. a service like email or a web page) with the intention that the target is breaking down as of the magnitude of simulations requests. Botnets are the preferable instrument for this type of attack.

[3] like intellectual property

[4] e.g. account or credit card information

[5] Hacktivism is an artificial word composed by activism and hacking. It refers to the conduct of malicious cyber activities by individuals or groups of them primarily to transport a political message rather than for monetary reasons (Denning 2001a).

the private sector – most of its banks, internet service providers and a number of news portals – suffered the disturbing effects of a cyber campaign. Among the methods seen, DDoS attacks against services reachable over the internet, defacing web sites or hacking against valuable targets, none of which were new or highly sophisticated or ultimately very damaging (Ottis 2008; Tikk, Kaska and Vihul 2010; Nazario 2009a). Botnets were again one major tool used for conducting many of the attacks.

While hacktivism and the use of botnets for political reasons has already been seen before 2007 (see e.g. Nazario 2009a), the strong media attention around this particular incident, classifying it as the first "cyber war" in human history (Landler and Markoff 2007), created cyber war hype (Farivar 2009) and with it fuelled subsequent hacktivist activities[6].

Since end of the 20th century, "Cyber" has become a prefix frequently used, sometimes without proper reflection, which has been added to existing terms like *attack*, *war* or *terrorism.* Nevertheless, this incident launched a discussion (still on-going) as to whether and in which way a cyber attack could be regarded as an armed attack in the context of the law of armed conflicts (see e.g. Schmitt 2002, 2012; Ziolkowski 2012; Wingfield 2006) and what role NATO could perform if any in such cases (McGee 2011; Dandurand 2011; Hyacinthe 2012).

Relevance of the Topic

States seem to have developed an increasing interest in the use of cyber means to support their interests, which is reflected in the dramatic increase of dedicated cyber strategies including the announcement of specialized forces to operate in cyberspace (see e.g. James A. Lewis and Timlin 2011; Cornish et al. 2010).

In addition, digital espionage entered its "Golden Age" (Geers 2011) as remote access to confidential information has become increasingly successful and less risky compared to the traditional means used so far (JA Lewis 2010; Reuters 2012). This has fuelled the creation of APT[7] actors being States, cyber criminals and industry (Command Five Pty Ltd 2011). The established population serves them as a new entry vector into highly secured targets of interest (GTISC and GTRI 2011).

Still the borders between cyber crime (which in most cases would include hacktivism) and terrorism, (cyber) war or espionage are hard to draw. From a

[6] See e.g. the raise of Anonymous (Pras et al. 2010; McLaughlin 2012)

[7] "*The term APT is commonly used in reference to the cyber threat posed by foreign intelligence services, or hackers working on behalf of such entities, but is not limited just to this and can equally be applied to other threat actors such as organised crime syndicates and those involved in traditional espionage."* (Command Five Pty Ltd 2011)

technological point of view, the technologies and techniques used for these different activities are mostly identical to and even overlap with those used for legitimate purposes in IT security or law enforcement. The intention behind the action is what ultimately determines the difference between activities that are technically similar. Attributing the real origin of a cyber attack, which would be necessary in many cases to identify the actors and their motivation, is commonly regarded as a difficult problem (Hare 2012; Applegate 2012; Nicholson et al. 2012).

The primary targets of most cyber attacks are business enterprises from all fields, which have to mitigate the damage they are suffering, either directly as the target of a cyber attack or as collateral damage (see e.g. at the example of UK in UK Cabinet Office and Detica Ltd. 2011).

States in the form of their governing institutions face very similar threats, and in addition, are targeted by threat agents from foreign States in the context of espionage or computer network operations.

Depending on the threat perceived or cyber attack experienced by each individual organization, managers at all different levels face the question of which actions to take and which resources to use to ensure business continuity. Larger organizations might already have an IT unit in charge of mitigating the threats posed by botnets, commonly applying a cyber crime risk management strategy, but their means are limited in the face of botnet attacks.

States have recognized these new threats and increasingly discuss their role in the cyber domain, especially from a military and national security perspective. This includes the protection of their critical infrastructure and national interests, including their economies, from the increasing impact of cyber attacks. Here, national security advisers and policy makers need to understand emerging new cyber threats along with the new actors behind them and have to agree on a policy on how to cope with them from a State perspective.

The interdisciplinary nature of the latest developments add to the complexity of the matter (Dunn 2005), and some argue that it is not yet sufficiently understood by policy makers for them to make good decisions (Cornish et al. 2010). From another perspective, there are voices warning against overreacting in the political response and overly focusing on high impact low probability risk scenarios (Cavelty 2012).

Research Aim and Question

The aim of the conducted research is firstly to support IT security managers, national cyber security experts and policy advisers, especially in government administration and military fields, to understand the changing role of botnets in the wider picture of cyber conflict. Secondly, it aims to explore the existing limitations

in countering botnets at the organizational level. Ultimately, this shall lead to developing a framework of State-level strategies and evaluating their effectiveness in mitigating the botnet threat, to the end that better informed strategic decisions can be made by the people in charge.

The research question is formulated as follows:

What are the best strategies that a State could use to enhance its national cyber security in particular against the threat posed by botnets in the context of the newly emerging realm of cyber conflict?

Cyber security is understood as the capability of a State to resist or mitigate the effects of cyber attacks against its interests and assets[8] in cyberspace by having appropriate means in place and supported by related legal, strategic and organizational frameworks.

Cyber conflict refers to a conflict between cyber-capable actors conducted primarily by means and tools unfolding their very effect in cyberspace. At least one party of the conflict is a State or an essential part of it so that the State would see any disturbance or damage to this part as a threat to national interests or sovereignty. It is up individual States to define their particular threshold.

This research was conducted under the assumption that the role of botnets have indeed changed, and that it is not enough to look at botnets solely from the cyber crime perspective. Further, it assumes that by fighting botnets – their development, spread and use – a significant contribution is made towards enhancing a State's cyber security. Finally, it is assumed (and supported in the course of the research later conducted), that an organizational-level response is not sufficient to effectively fight the botnet issue and that a State-level approach is necessary for this.

Research Tasks and Main Methods Used

To develop an answer to the research question, a set of research tasks was formulated and individually answered. Key findings were published in **Publications I to V.**

Firstly, in accordance with the idea of strategic planning, it was necessary to understand the external environment with its landscape of threats, which challenges decision-makers as they need to understand and make wise decisions.

To this end the *first research task* was to explore the nature of cyber conflict and in this context the means of malicious activity. System analysis techniques were used to identify the unique features of cyber weapons together with a definition of them.

[8] This extends from the protection of its citizens from foreign influence or crime, industry and economic interests and ends with the governing institutions and critical infrastructure.

These findings were further developed into a new model to describe cyber conflict and the special role vulnerabilities in soft- and hardware play within them. The key findings were presented in **Publication I**.

The *second research task* aimed to understand the current role of botnets in cyber conflict. It was assumed that their role has changed over the last decade from being primarily a cyber crime related tool towards becoming an important type of cyber weapon that a variety of different actors are taking advantage of to pursuit their goals. This includes new actors using botnets, new motivations, new ways of infection and new features implemented by botnet technology. In the course of this research task, system-mining techniques were applied to systematically discover these changes based on past events, and this led to the development of the taxonomy presented in **Publication II**.

With the wider context explored, the *third research task* was to understand the opportunities and limitations for IT security managers and practitioners at an organizational level to cope with the effects caused by botnet mounted attacks. For this, the current state of the arms race between those developing or using botnets and those trying to take them down was explored conducting case studies and interviewing experts conducting these take downs on a daily basis. This research focused on such resources as *time*, *skills* and *money*. As botnets can be used to conduct some types of attacks where a proper defence against them is currently not possible, it was of particular interest whether a tactical, meaning timely, takedown of a botnet is possible and feasible. The findings are presented in **Publication III**.

With the wider context explored and the limitations of an organization-level response against the botnet threat identified, the *fourth research task* was to firstly identify the strategies a State can implement to enhance its cyber security and with this its resilience against botnet mounted attacks. As Estonia was reported to be the first State suffering from massive cyber attacks and as such has identified some concrete lessons learned back in 2007, a case study on the changes in Estonia three years after the attacks was conducted and presented in **Publication IV**.

These findings were extended and generalized into a framework of 10 groups of strategic options for States to mitigate the botnet threat. This is part of **Publication V**.

Furthermore, the research also aimed to evaluate the strategic options it identified in terms of their effectiveness. Based on the empirical material collected and through the application of an established method called DEMATEL for finding solutions in complex decision-making situations, an influence model was created. This made it possible to analyse and rank the strategies in terms of their performance. The findings were presented in **Publication V**.

Originality of Research and Its Practical Merit

The field of research into cyber conflicts is developing but still there is a lack of established terminology and understandings and principles, especially in relation to the dimension of warfare and terrorism.

Over the last decade, botnets already received attention in the cyber crime context (Council of Europe 2001; European Commission 2010; OECD 2008; Eeten et al. 2010), but it is assumed that this is still insufficient for current requirements, as new actors continue to join the established ones using botnets to satisfy their (different) needs.

Further, while recommendations have been made on how to mitigate the botnet threat (see e.g. Anderson et al. 2008; Plohmann, Gerhards-Padilla and Leder 2011; Eeten et al. 2010), they often do not apply a method to rank these recommendations in terms of their impact or efficiency.

One of the few exceptions is Geers (2011), who in discussing high-level strategies, such as deterrence, arms control, development of doctrines and investment in new technology, so a State could mitigate cyber attacks in general, managed to form a ranking of these strategies.

This research sees its main contribution as follows:

- Firstly, it adds to the body of knowledge in the field of cyber conflict research by offering new models and delivering new insights into the nature of cyber weapons and the consequences for those involved in cyber conflict.
- Secondly, the changing role of botnets is captured in a newly developed botnet taxonomy centred on usage.
- Thirdly, it delivers a comprehensive and up-to-date framework of State-level botnet mitigation strategies.
- Fourthly, by applying the established DEMATEL method on empirical expert knowledge, an evaluation of these strategies is conducted to enable a justifiable recommendation of which strategies to prefer.

PART I. THE THEORETICAL BACKGROUND FOR ANALYSING STATE-LEVEL BOTNET MITIGATION STRATEGIES

Cyber conflict research is a relatively new domain of research emerging from a number of different fields such as military science with regards to the principles and strategy of warfare, computer science for the technological basics of the tools and methods used in cyber conflicts as well as political science (Ottis 2011).

Management science is involved on different levels and with different scope, but generally where available resources (i.e. human resources, knowledge, money and time) need to be applied efficiently. This is true on the tactical level, where IT security and risk management on an organizational level in the private and public sector alike are challenged to mitigate the impact caused by botnet attacks. This is also true on a national or State level, when States have to solve the problem of identifying, evaluating and deciding upon proper strategies to enhance their cyber security framework with regards to the threat posed by all types of cyber attacks including those mounted by botnets.

For managers and policy advisers to make informed decisions, it can be necessary to look at the threat posed by botnets from independent positions and fields of research.

Firstly, the technology behind botnets should be explored to understand the possibilities as well as limitations of managing the risk posed by botnet mounted attacks and to understand and evaluate the countermeasures possible. This primarily draws from the field of IT security, being part of computer science.

For managers to understand the wide context in which they have to operate, a second view looks at the cyber security dimension of the botnet threat. Here, the changing role of botnets as one of the main tools for various actors in recent cyber incidents and conflicts needs to be recognized to understand the motivation behind new and old malicious activities as something managers on an organizational level and policy makers on a national level have to cope with.

And finally to bring this understanding in to operational practice, managers and policy makers alike have to conduct strategic decision-making processes to appropriately address and respond to the threat posed by botnets.

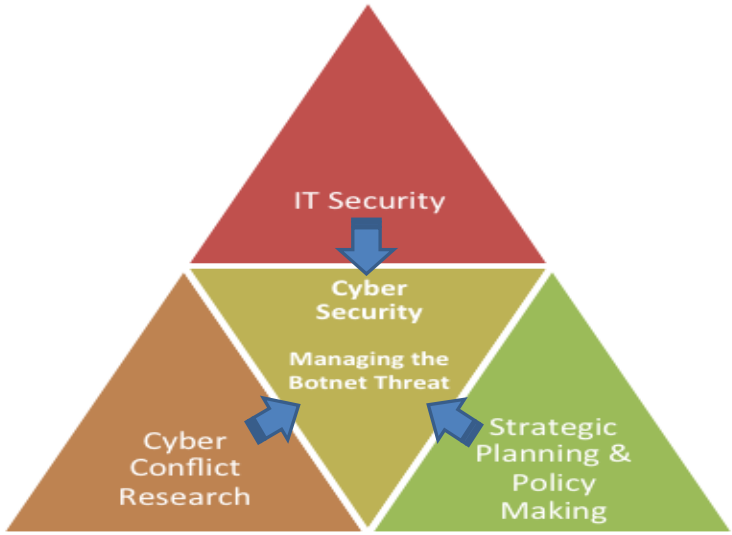

Figure 1. Interdisciplinary approach to managing the botnet threat (compiled by the author)

I.1 IT Security View of Botnets

To fully understand the reason behind the current threat posed by botnets, it is important to understand the technology behind them.

A botnet consists of a typically advanced piece of malware[9] widely distributed with the crucial feature that it can enable remote control over the infected system by establishing and maintaining a communication channel to a Command and Control (C&C) infrastructure established by the botnet's creator. A victim system infected in this way is commonly referred to as a bot, short for robot. If this scheme is utilized on a larger scale, a network of hijacked systems is formed and centrally controlled by its creator (Plohmann, Gerhards-Padilla and Leder 2011). Most infected systems are end-user devices with a high speed internet connection; on average, botnets have a life time of several months before they die or are replaced by a subsequent generation (Thonnard, Mees and Dacier 2009).

While the very first versions of botnets were made for fun and as a display of skill among peers in the early eras of the "hacker community", the level of sophistication and implemented functionality has changed in recent decades along with the rise of organized cyber crime (Plohmann, Gerhards-Padilla and Leder 2011; Kola 2008).

[9] *Malware* is an artificial word created from "malicious software" and refers generally to all sorts of software executed on an infected computer system without its owner's knowledge and consent. Mostly it has an economic or privacy damaging effect.

The first version of malware used to create a botnet was called *Eggdrop*[10] – first seen in 1993. Among the first functions implemented was the capability to conduct (D)DoS attacks (Plohmann, Gerhards-Padilla and Leder 2011).

Throughout the history of malware, difference methods for infecting and spreading were invented, resulting in various names for malware like *trojan*, *worm* or *virus* (Plohmann, Gerhards-Padilla and Leder 2011). While taxonomies of malware have been developed over time (see e.g. Dagon et al. 2007; Rutkowska 2006; Kirillov et al.), current malware, and in particular those used for botnets, are commonly hybrids, combining and merging different spreading techniques and implementing rootkit technology[11] to hide themselves and often come with an update functionality allowing them to add new or improve existing functionality. This makes these classifications hard to apply nowadays. A botnet is de facto only limited by the creativity and skills of its developer and the performance of the infected systems.

The most common cases of botnets are spamming, information theft, hosting malicious services, disguising malicious actors and their services, and performing distributed denial of service attacks (OECD 2008).

To control a botnet, its creator needs to set up a control instance commonly referred to as a Command and Control server (C&C). Here different architectures have been developed over time; many increase their resistance towards takedown attempts. A more technical overview is provided in, for example, (Plohmann, Gerhards-Padilla and Leder 2011; Leder, Werner and Martini 2009).

Furthermore, the abuse of legitimate services like Google Workgroups (Perez 2009), Twitter (Nazario 2009b) and Facebook (Lelli 2009) has been seen, although this method has not become widespread yet.

It is important to note that well deployed botnets distribute their C&C server infrastructure over multiple countries and often prefer those where malicious cyber activities are not criminalized, insufficient law enforcement structures are present or data protection and privacy regulations delay quick takedown attempts (Leder, Werner and Martini 2009; Plohmann, Gerhards-Padilla and Leder 2011). Further, by introducing P2P technology into bot malware, every single bot in a botnet can be utilized as a C&C server effectively distributing this functionality all over the botnet. Figure 2 illustrates this *pars pro toto* using the example of Conficker, one particular botnet which drew global attention in 2009.

This is one major part of the problem currently faced in an effort to mitigate botnets.

[10] This bot is still around and available under the GNU General Public License at http://www.eggheads.org/

[11] The term *root kit* refers to the ability of software to hide its presents from the operating system by hooking into core components of it in a way that detection becomes close to impossible.

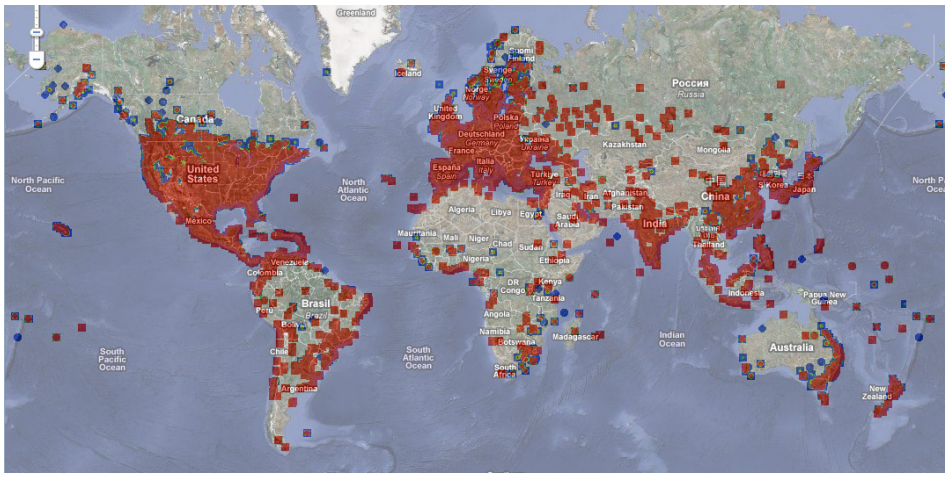

Figure 2. Global Conficker infection as of April 2009. (Source: Conficker Working Group 2009)

Furthermore, since the end of the 20th century, there has been a shift in the professionalism of cyber crime actors (Brenner 2002; Berg 2007), and with this, botnet developers (see e.g. Herley and Florêncio 2010; Steigerwald et al. 2011; Stone-Gross et al. 2011). Organized (cyber) criminals are applying the latest software development and quality assurance methods to develop secured botnet software. They actively track new detection techniques quickly, developing appropriate counter measures and experiment with new ways for hardening the C&C structures against takedown, or hiding communications from detection (Klein, Leder and Czosseck 2011; Plohmann, Gerhards-Padilla and Leder 2011; Iland 2010). An underground economy has emerged, selling sophisticated botnets in the form of easy to use botnet kits, providing maintenance, update and customer support services like common for legitimate software.

In response, those defending against such attacks are mainly the developers of antivirus and IT security software, companies specialized on botnet mitigation as well as security research and activists, mainly from an academic or voluntary background, trying to fight the overwhelming armies of botnets.

I.2 Strategy Management and Policy Making

The idea of strategy or strategic planning in its very origin is grounded in the art of warfare reaching back to the ancient Greeks, where *stratego* means to "plan the destruction of one's enemies through the effective use of resources". While there are ancient examples from the application of strategy in a business environment, it took until the Industrial Revolution for the concept of strategy to be re-introduced to business (Bracker 1980).

According to *Igor Ansoff*, this change is attributed to two significant factors, firstly the increasing speed of market changes, challenging companies to focus; and secondly, the accelerated application of technology and scientific progress (Bracker 1980). Bracker provides a comprehensive review of the historical developments of strategic management and attributes the first modern reincarnation of strategic planning to the theory of games, developed by Von Neumann and Morgenstern back in 1947. In the decades that followed, numerous other authors turned their attention to strategic management and offered their definition of strategic management, including but not limited to Andrews (1980), Chandler (1993), Porter (1996) or Bryson (2004). Bracker (1980) e.g. writes "*The major importance of strategic management is that it gives organization a framework for developing abilities for anticipating and coping with change.*"

Hofer (1978) presented a comparison of many of these definitions of strategic management, identifying three major fields of differences between them: a) the extent covered by the concept of strategic management defined, b) the components identified as essential for a strategy and c) the extent to which a strategy-formulation process was included. Bracker (1980) extended this by identifying the similarities of the same main group of authors, being an environment or situational analysis as well as a consideration of a firm's resources. Mintzberg, Ahlstrand and Lampel (1998) developed a framework of Ten Schools of Thought to structure the different views on strategic management.

All this leads to the insight that there is currently no clear widely-accepted definition present, "*[o]nly different views and opinions offered by different writers working different agendas*" (Nickols 2011).

Crosby and Cleveland (1991) describe four essential elements of strategic management being a) an orientation toward the future, encouraging anticipation of an overreaction to changes; b) an emphasis on external influences; c) a focus on assuring a good fit between the environment and the organization, taking future changes into consideration by continuously re-assessment and adaption; and finally, d) by understanding the strategic approach as a continuous, repeating process.

This process can have different forms and stages. Many authors have presented their systems – among them, Bozeman and Straussman (1990), White (1990), Young (1995) or Bryson (2004).

Figure 3 illustrates Bryson's process *pars pro toto*. As there exists nuances in the understanding of strategic management by different authors, the same holds true for the processes proposed by them.

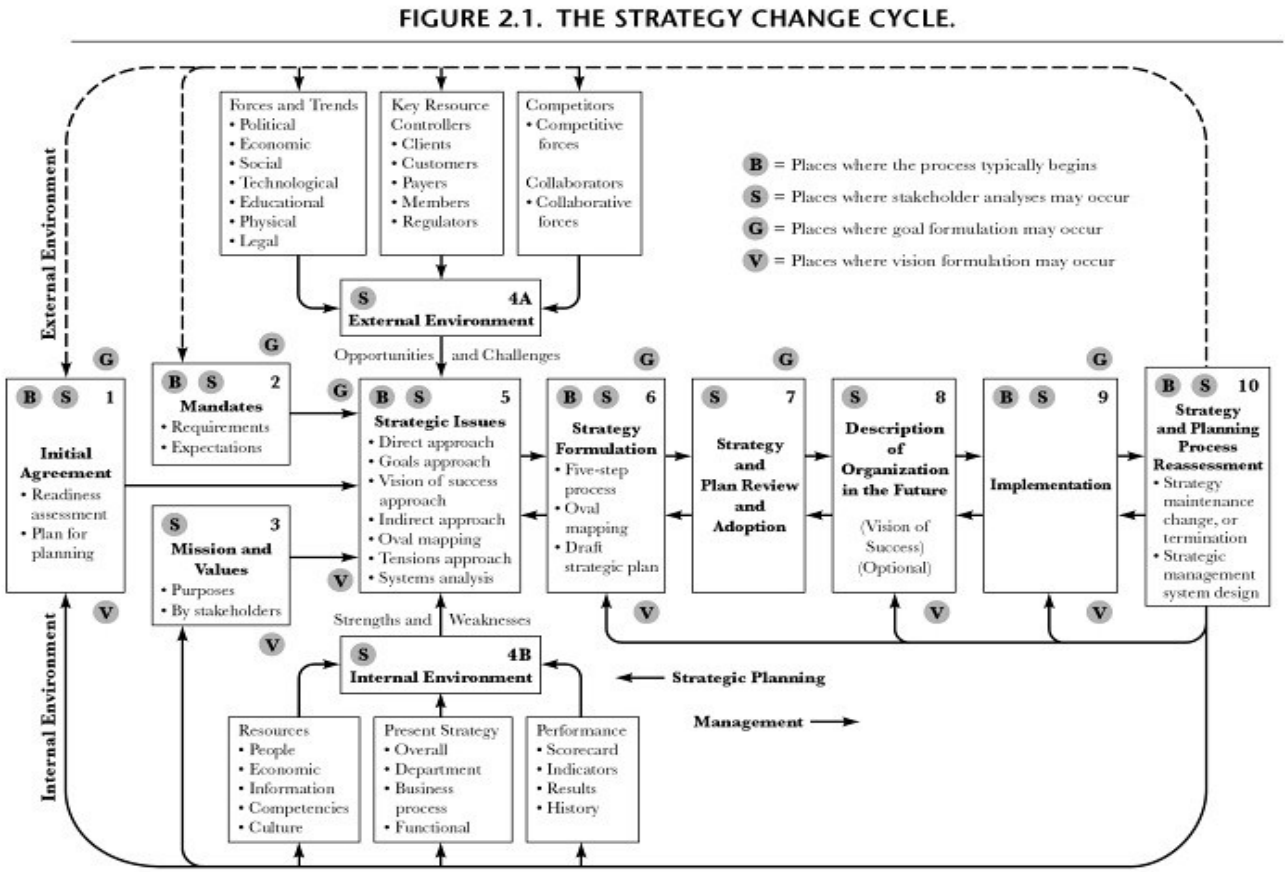

Figure 3. The Strategy Change Circle taken from Bryson (2004, p. 33)

Often, the main differences lie in the final steps, whether they include implementation and monitoring or not (Crosby 1991). To its very core, all these processes have five essential parts: 1) Goal-setting; 2) Analysis; 3) Strategy formulation; 4) Strategy implementation; and 5) Strategy monitoring (Scribner 2000) as illustrated in Figure 4. But this again is not universally accepted. Young (1995), for example, offers a different view by identifying vision, assessment, strategies and measurement as the essential elements. In the end it is up to the organization or strategic manager to decide which elements to include.

Figure 4. Strategic Management Process according to Scribner (2000)

The challenge of coping with change is not unique to the private sector. *"[O]il crises, demographic shifts, changing values, taxing limits, privatization, centralization or decentralization of responsibilities, moves toward information and service-based economies, volatile macroeconomic performance"* (Bryson 1988) are many of the main drivers for the adoption of business management techniques by public and non-profit organizations (Bryson 1988; Wechsler and Backoff 1986). Its very origin can be traced back to the early 1960s, as the US Department of Defense started to explore ways for better long-term planning (Young 1995). In addition to discussions on governance, this all came together under the heading New Public Management (Klijn and Koppenjan 2000).

Still, as public organizations operate on a different basis, they are not driven by market competition rather they *"act within relatively complex, multilateral power, influence, bargaining, voting and exchange relationships."* Public agencies are restricted by the national legal framework, the mandate given to them and resource constraints, but also political influences and rules established by the current government. Strategic choices and performance does not only occur through a single agency, but often requires inter-agency coordination and consolidation (Wechsler and Backoff 1986).

As Drechsler (2005) elaborates, current research sees New Public Management on the back step at best, or even failed, as empirical findings have come out clearly against it; yet it still seems to be alive in many areas.

Policy making is one of the core instruments for a government to exercise its role within a State. It is first of all an inherently political process, which can be characterized by two major phases: political and technical as illustrated in Figure 5 (Health Sector Reform Initiative 2000).

Updating national security strategies by including a perspective on cyberspace, as has increasingly been witnessed in recent years (Jellenc 2012; James A. Lewis and Timlin 2011), is a regular policy making activity, not different from others. Still, policy making is often an issue- or threat-driven process (Dunn 2005; Health Sector Reform Initiative 2000).

The 2007 cyber attacks against Estonia might have served as such a trigger for many States to bring cyber security onto the political agenda. As Cavelty (2012) elaborates, it is possibly an overreaction to put too much emphasis on catastrophic scenarios that are highly improbable and further assume too much regulatory influence a State might execute in cyberspace at all.

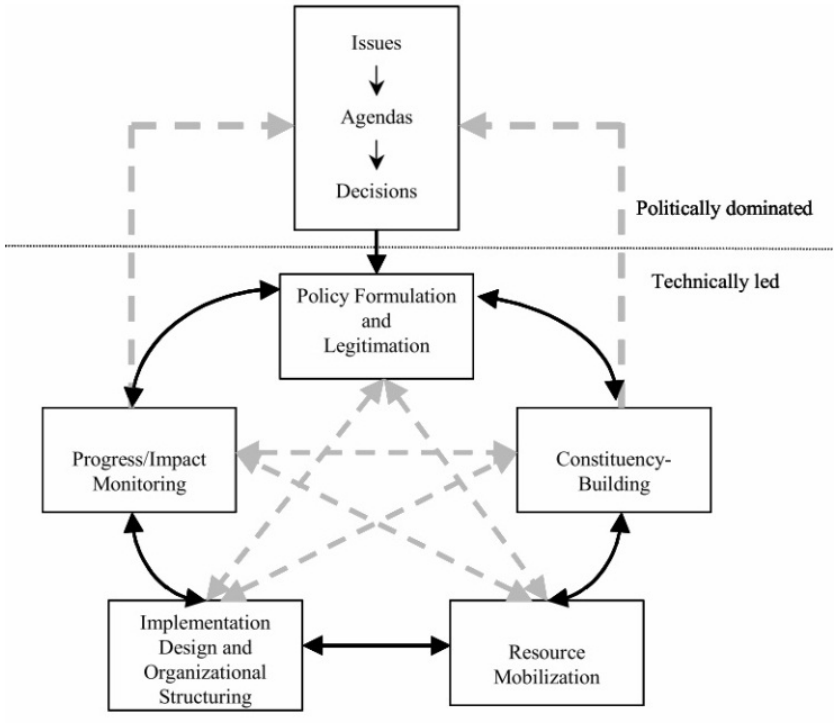

Figure 5. The Policy Process taken from (Health Sector Reform Initiative 2000)

Publication V adds to this discussion by presenting a framework of strategies and by successfully applying an established multi-criteria decision-making method in a new context being the mitigation of the botnet threat.

I.3 From CIIP to Cyber Security

The mid-1990s shift from seeing information infrastructures primarily as a tool for obtaining competitive advantage (especially in the business world) towards recognizing national dependency on (critical) information infrastructures as a national interest, ultimately brought the protection of (critical) information infrastructures (CIIP) to the agenda of security policy as elaborated by Dunn (2005).

Cyber security as a "sequel" to CIIP rapidly entered the agenda of national security circles forcing States to re-evaluate their national security frameworks.

One key event for this can be seen in the cyber attacks against Estonia in 2007 being (too) quickly labelled the first *cyber war* in history (Landler and Markoff 2007), and followed by hyped media attention towards all sorts of cyber incidents (Farivar 2009). Another can be seen in the increased use of cyberspace and especially the internet by States for conducting (digital) espionage at the end of the 20th century (JA Lewis 2010; Reuters 2012). And lastly, in the increasing numbers of cases of hacktivism with its increasing impact on foreign policy as seen in the example of Anonymous and WikiLeaks (McLaughlin 2012; Denning 2001a; Tikk, Kaska and Vihul 2010; Ludlow 2010).

Already before the Estonia incident, some argued that the concept of cyber security had been (artificially) raised as a national security debate (Nissenbaum 2005). And more critical voices were heard afterwards, challenging the cyber war rhetoric (JA Lewis 2010) or the use of threatening worst-case scenarios for policy decisions (Cavelty 2012; Cavelty 2008).

There is no commonly accepted definition for the term cyber security.

Ottis (2011) understands it as an evolution over time connecting established computer and data processing related fields, such as data protection, IT security, or Information Assurance along with political and military science and bringing them all to the State level.

Alternatively, Hare (2010a) understands cyber security as:

> The state of being in which the populace, governing institutions and critical infrastructure are not threatened by:
> - attacks and intrusions through cyberspace, by either state or organized non-state actors, against government and select other information systems to gain knowledge of a national security value

- attacks and intrusions through cyberspace, by either state or organized non-state actors, against critical infrastructure systems (privately and publicly owned) to degrade or disrupt such systems creating a national security crisis.

Building on the idea from Hare, this research understands cyber security as the capability of a State to resist or mitigate the effects of attacks against its interests and assets[12] in cyberspace by having appropriate means in place supported by related legal, strategic and organizational elements.

Policy makers in general were forced to respond to these rapid changes under the additional pressure of hyped media attention, and some scholars have argued that in general they did not understand the problem well enough to come to an informed decision (Cornish et al. 2010). Others pointed out that there is no consistent opinion on this problem between States to start with (Hare 2010b).

The Cyber Security Response at State Level

The years after the cyber conflict in Estonia saw many western States issue dedicated cyber security strategies, which they had not done until this point, with a few exceptions (see e.g. Dunn 2005; Jellenc 2012; James A. Lewis and Timlin 2011).

Estonia issued its very first strategy in 2008, responding to the cyber attacks with comprehensive changes to their legal, organizational and strategic framework. This was subject to a further analysis conducted in **Publication IV**. In the following years many more were to follow introducing new or revised cyber security strategies (e.g. Australia and Great Britain in 2009, Canada and Japan in 2010, France, Germany, The Netherlands, The Russian Federation and The United States of America in 2011 and South Africa in 2012)[13]. A recent overview and brief comparison is provided in Jellenc (2012).

The Cyber Security Response from International Organizations

Beside States, international organizations also responded to these changes and issued cyber strategies for coping with them.

The European Union is currently in the process of formulating a strategy and has published the *Proposal on a European Strategy for Internet Security* expected to be adopted at the end of 2012 (European Commission 2011a). Under separate

[12] This extends from the protection of its citizens from foreign influence or crime and includes its industry and economic interests and ends with government institutions and critical infrastructure.

[13] A selection of these strategies is presented by the NATO CCD COE webpage at http://www.ccdcoe.org/328.html

cover and in continuation of existing activities related to cyber crime and critical infrastructure protection, a series of communications and directives were prepared and initiatives launched such as the *EU initiative on Critical Information Infrastructure Protection* (Council of Europe 2005; European Commission 2007; European Commission 2011b) or the European Public-Private Partnership for resilience programme[14] (European Commission 2010).

Similar initiatives are on-going within the OECD (Eeten et al. 2010) and to a limited extent at the United Nations (Sidorenko 2011; United Nations 2011).

NATO already suffered cyber attacks in the late 1990s during the Kosovo conflict, when a pro-Serbian hacker attacked NATO web sites[15], and the need to establish defensive cyber capabilities became apparent. With the 2007 cyber attacks on Estonia, they received the second wake-up call realizing that it also needs to be concerned about the cyber defence of its member nations (McGee 2011; NATO Parlamentary Assembly 2009).

The first step was a new Policy on Cyber Defence approved in 2008 at the Bucharest Summit (NATO 2008) and the second, NATO's revised Strategic Concept in 2010, where NATO and its member nations recognized cyber attacks as:

> becoming more frequent, more organised and more costly in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability. (NATO 2010)

This was followed by the revised Policy on Cyber Defence in 2011 (NATO 2011) accompanied by a frequently updated Cyber Defence Action Plan.

The Cyber Security Response from Industry

In an effort to mitigate the increasing damage caused by malicious cyber activities in general, and with it, botnet mounted attacks as one of the major issues, industry independently and in cooperation with States has become increasingly active in recent decades.

Many new public-private partnership programmes and industry initiatives were formed and prominent examples include end-user awareness and support projects like the Japanese Cyber Clean Center launched in 2006 (CCC 2011) or the German

[14] With a dedicated working group on botnets.

[15] As one core response, NATO established the NATO Computer Incident Response Capability (NCIRC) at the 2002 Prague Summit to detect and prevent cyber attacks against NATO.

Anti-Botnet-Advisory Centre launched in 2010 (ECO 2011). Furthermore, voluntary collaboration among internet service providers (ISPs) with or without government support has been promoted since the middle of the 2000s, receiving a boost in recent years. Examples include the Australian Internet Security Initiative since 2006 (ACMA 2005) or the Dutch anti-botnet MoU between ISPs signed in 2007 (Evron 2009).

In addition, private sector and security researchers are getting more organized and collaborative, launching different initiatives to take down botnets on a global scale. Microsoft's efforts through its Digital Crimes Unit (Microsoft 2011) in coordinating and taking down major botnets like Rustock (Fisher 2011) or Waledac (Fisher 2010) is a remarkable example of this.

I.4 Cyber Conflict and the Role of Botnets

As Adkins (2001) describes, "[The] *spectrum of cyber conflict ... consist*[s] *of various forms of cyber attack such as hacking, hacktivism ..., espionage, terrorism, and information warfare."*.

For this thesis, *cyber conflict* is understood as an event or series of events between cyber-capable actors[16] conducted primarily by means[17] unfolding their very effect in cyberspace[18]. At least one party in the conflict is either a State or an essential part of it so that this State would understand disturbance or damage to this part as a threat to national security, interests or sovereignty. It is up the individual States to define their particular threshold.

As with previously well-defined types of conflict, cyberspace adaptations have been established by adding "cyber" as a stem to modify classical terms describing types of conflict (Lorents and Ottis 2010). In the discussions that follow, three are of particular interest: *cyber terrorism*, *cyber war* and *cyber crime,* which all represent important threats or risks to a State's cyber security.

The potential threat of *cyber terrorism* has been raised by some scholars (Charvat 2009; Janczewski 2008), but for the moment no commonly recognized cases of cyber terrorism[19] have been conducted (Cavelty 2008). Some argue that it might only be a question of time before this happens, and States are encouraged to consider this threat as forthcoming (Chu, Deng and Chao 2009).

---

[16] Be it individuals, groups, private or public sector organizations or States

[17] This includes in particular the use of hacking techniques or malware.

[18] The effects caused are primarily of digital nature; this does not rule out the fact that there is a real world effect as a direct consequence of cyber activities.

[19] Meaning the cause of death and destruction as well as the spread of terror and fear exclusively by cyber means. This does not mean terrorism related activities like fund raising, recruitment or the lone use of information and communication technology for establishing communication between terrorists.

Cyber war, on the other hand, is a frequently used term especially by the media (Farivar 2009) since the Estonia incident in 2007, indiscriminately using this term to refer to all sorts of malicious activities in cyberspace, paying little attention to the established meaning of the term *war*.

In all cases seen so far, real cyber war has not taken place (JA Lewis 2010). Instead most actions currently seen and conducted by individuals or groups of individuals are, from a legal point of view, to be classified as *cyber crime*. This also includes cases of hacktivism, cyber attacks by individuals conducted with a political rather than a monetary motivation. As such, the use of the term "war" is rather misleading and the activities seen, for example, in 2007 have officially been regarded as an act of crime rather than war (Tikk 2009).

The criminalization of certain malicious activities (which commonly includes cases of terrorism) is a matter of national criminal codes and law enforcement. Because of the increasingly transnational nature of organized cyber crime, international efforts are being made to harmonize criminal codes and to enhance the transnational fight against crime. In addition to many existing bi- and multi-national agreements, the Council of Europe Convention on Cyber Crime (Council of Europe 2001) might be most noteworthy. In addition to most European Countries, Canada, Japan, South Africa and the USA have signed the convention. As of 2012, 33 States have ratified the convention, 14 more have signed it and more than 100 nations worldwide are said to use the Convention to strengthen their own legislation using it as a guideline or "model law" (Council of Europe 2012).

Correctly positioning *cyber war* requires acknowledging the body of laws governing *war* and with it *armed conflict*. This body is broadly divided into two groups: *jus ad bellum*[20] and *jus in bello*[21] with the latter commonly referred to as the Law of Armed Conflict (LOAC) or International Humanitarian Law (IHL).

While there is an established practice when it comes to "old" types of armed conflict, it is currently unclear to which extent a *cyber war* could be possible in this legal framework, and whether the existing framework is sufficient to cover such instances.

The Manual on International Law Applicable to Cyber Warfare[22] is expected to support this discussion by offering its interpretation and guidance. Among others, it requires a cyber attack to have an equivalent level of impact to respective conventional activities before it could be considered *use of force* or an *armed attack* in the sense of these two legal terms. Up to this point there has not been any case of a cyber attack commonly regarded as having passed this threshold.

---

[20] Jus ad bellum is the "body of international law governing the resort to force as an instrument of national policy" which could lead to an armed conflict (Schmitt 1999).

[21] *Jus in bello* is understood as the "body of law concerned with what is permissible, or not, during hostilities, irrespective of the legality of the initial resort to force by the belligerents"(Schmitt 2002).

[22] expected for beginning 2013, see www.ccdcoe.org/249.html

What has been seen is the use of cyber means along with the use of force in the form of conventional weapons in the conflict between Russia and Georgia in 2008 (Tikk, Kaska and Vihul 2010), while latter has been the deterministic factor in declaring this incident as an armed conflict.

The Militarisation of Cyberspace

While some scholars have raised warnings about cyberspace turning into an unregulated playground for power games or even conflict between States, suggesting an international effort to put a global governance of cyberspace in place before his happens (Hughes 2009), the recent past has shown a different development.

Many States currently seem to see it as an advantage to have a more or less unregulated cyber war/conflict domain to provide them with room to explore new ways of projecting power and supporting their interests (Fritz 2008). Libicki (2009) introduced the idea of sub rosa cyber war, where nations are expected to enter a silent confrontation without publicly acknowledging it. This idea is supported by other scholars arguing that the cyber domain might have the power to rise from a role as a force multiplier to become a fundamental part of a State's power multiplied by conventional means (Amit Sharma 2009). Liles introduces the idea of low-intensity conflicts, were States attack each other via a series of (individually taken) insignificant cyber attacks, which added together likely have a significant effect on the opponent, especially its economy (Liles 2010), and Watts takes this idea up and concludes that this type of strategy is unlikely to trigger LOAC mechanisms (Watts 2011).

Further, cyberspace became officially declared the 5th domain of war after land, see, air and space by the USA and Canada (Starr, Kuehl and Pudas 2010), and many States are setting up specialized structures for military operations in cyberspace.

Billo and Chang (2004) offer a comparison of the cyber doctrines or equivalent documents for China, India, Iran, North Korea, Pakistan and the Russian Federation as far as back in 2004. Public information is available for 2011 about 33 States that have included cyber warfare in their military planning and organizations; an overview is presented in J. A. Lewis and Timlin (2011). In addition to USA, China (Krekel, Bakos and Barnett 2009; Perry 2007; Kanwal 2009; Fritz 2008) and Russia (Giles 2011; Giles 2012) are known for being well advanced in developing cyber warfare capabilities.

The earliest documented examples of the use of cyber means by States go back to 1982 when a logic bomb was planted in gas drilling equipment stolen by the KGB, which ultimately led to a sizeable explosion in Siberia (Russell 2004; Safire 2004), or US plans for a cyber attack along with their conventional operations taking place back in the first Iraq war. Gordon (2008) has discussed "Cyber Weaponization"

and Jellenc (2012) recently confirmed an arms race having started in and about cyberspace.

Publication I adds to this discussion by presenting a definition of cyber weapons along with a discussion and justification of their unique features and developing this further into a model of cyber conflict.

State use of Botnets

Among the means used by some States, botnets are used, for example, to enforce censorship on media and news portals in peace time (Pavlyuchenko 2009; Nazario 2009a), but also in time of conflict (Tikk, Kaska and Vihul 2010). Botnets are used in the context of State-driven espionage and are reported to serve as a new entry vector into highly secure targets (GTISC and GTRI 2011). Furthermore, some States seem to explore options for using hacktivists and cyber criminals to pursue national interests by providing tools, guidance or protection, but leaving the execution of the cyber attack to them, consequently being able to deny responsibility for the attacks. China's Information Operations doctrine even explicitly introduces the idea of a "People's War" (Marquand and Arnoldy 2007).

The cyber attacks against Estonia in 2007 or the military operation in the 2008 Georgia-Russian conflict, which seemed to be coordinated with cyber attacks by cyber criminals and hacktivists, serve as examples (Tikk, Kaska and Vihul 2010).

Still, acts of hacktivism are increasingly conducted without guidance from States and the amplification power of the internet empowers these mere individuals to express their political opinion to the extent that does concern States. The actions of the group *Anonymous* (and their off-spring *LulzSec)* (Mansfield-Devine 2011; McLaughlin 2012) as well as *WikiLeaks* (Correll 2010; Pras et al. 2010; Ludlow 2010) serve as well-known examples here. Gandhi et al. (2011) recently presented a comprehensive overview of cyber attacks since 1998, classifying them in terms of social, political, economic and cultural motivation. Botnets, in terms of their ability to launch DDoS attacks, are the primary tools for them as a review of recent politically motivated cyber attacks shows (Nazario 2009a; Pras et al. 2010).

This all illustrates the important role of botnets in the current (cyber) threat landscape and their impact on national security and interests.

PART II. THE EMPIRICAL RESEARCH OF BOTNETS IN THE CONTEXT OF CYBER CONFLICT

II.1 Composition of the Research Project

The research aims to support IT security managers, national cyber security experts and policy advisers – especially those in the government administration and the military – concerned with enhancing a State's national cyber security so they can make informed decisions. In terms of the complexity of this subject and in light of the 2007 cyber attacks, this research limits its focus to the role of botnets as one major instrument for conducting malicious cyber activities. It assumes that:

a. Botnets, among all recent forms of cyber attacks, represent a sufficiently important tool for conducting cyber attacks, even though not all cyber attacks use them. Means to reduce the threat posed by botnets will also have a positive effect on the resistance against all other types of cyber attacks;
b. Reducing the botnet population results in enhanced cyber security;
c. The role of botnets has changed from being primarily a tool for cyber crime to become an instrument that is also used for military, espionage, crime and politically motivated usage alike;
d. Defence against botnet attacks at the organizational level is a difficult or even impossible challenge;
e. Properly set up and maintained botnets are hard to take down as their herders will take advantage of globally distributed C&C infrastructures and legal grey zones;
f. Every modern State suffers from cyber attacks to a varying extent and has at least recognized its dependency on IT and access to the internet.

The government administration of nations aiming for a comprehensive approach to enhance their cyber security in order to – among others – mitigate the impact of cyber attacks, and with it those mounted by botnets, are required to identify and evaluate valid strategies. This motivates the formulation of this dissertation's research question as follows:

What are the best strategies that a State could use to enhance its national cyber security in particular against the threat posed by botnets in the context of the newly emerging realm of cyber conflict?

In the course of research conducted to answer this question, multiple *research tasks* were identified and individually satisfied in the form of dedicated, published research papers.

Following the principle of the strategic planning process, one essential step is to understand the external environment. The **first research task** was to develop

a better understanding of the special nature of cyber conflicts, and with it the changes in the threat landscape that States and organizations alike confront in the 21st century. A particularly narrow area was identified, which was to focus on the role of the vulnerabilities in the power struggles between cyber actors, and further, to explore the nature of cyber weapons with presumably new or unique features.

As such this research task *(RT1)* was defined to answer the question: *What is the nature of cyber weapons and to what extent does this differ from the established principles of conventional arms and warfare, and further, what are the implications for cyber conflict?*

Publication I was dedicated to answering this question using primarily system analysis techniques. After presenting its own definition of cyber weapons, a discussion of the similarities and differences of cyber weapons compared to conventional weapons was presented. Focusing on the role of vulnerabilities, a vulnerability-based model of cyber conflict was developed and presented, enabling an analysis of the relationship between cyber-capable actors such as nations.

In the second step to analyse the external environment in order to answer the research question, it was necessary to reach an understanding of the role botnets play in current cyber conflicts.

Recent cyber incidents of major importance showed many (especially emerging) actors increasingly using botnets as a tool of choice to achieve their goals. It was assumed that this development challenges the established understanding that botnets are primarily an instrument for illicitly acquiring money.

As such the **second research task** *(RT2)* was defined to answer the question: *What is the current state of botnet usage?*

Using primarily data and system-mining techniques, cases of cyber incidents from the recent past (where botnets were used as the main instrument) were analysed and resulted in the development of a usage-centric botnet taxonomy that was presented in **Publication II**. This taxonomy, in contrast to previous work, does not focus on technological aspects but provides a holistic view by also including actors, their motivation and expected outcome.

As in the analysis of the internal environment of the strategic planning process, and understanding that a one-suit-fits-all analysis was beyond the scope of this research, it was necessary to discuss the principal relationship between offenders and defenders in the case of a cyber attack using botnets. Here the focus was on the resources needed to develop, acquire and use, on the one side, and to defend against this type of attack on the other. In terms of the defence against these attacks, acknowledging the limitations in terms of the options for defending against on-

going botnet attacks[23] and the resources necessary for a tactical take down[24] were of particular interest.

The **third research task** *(RT3)* was set to find an answer to the question: *What resources (in terms of skills, time and money) are required to set up a botnet compared to those needed to take one down.*

Publication III was the result of this research task. Based on the analysis of multiple botnet takedowns (case studies) in the recent past, and an in-depth investigation of various botnet architectures, the paper presented a classification of botnets on the basis of their level of sophistication and a discussion of common countermeasures.

In the analysis presented, special focus was placed on resources in term of the *time*, *skills* and *money* needed for each type of botnet and each stage in its life cycle – development, acquisition, use, defence and takedown. This included a limited discussion of the legal and ethical questions related to these countermeasures.

This research especially addresses government administrations in their effort to enhance the national cyber security of a State, as formulated in the research question.

Following the strategic planning process further as a guide, the **fourth and final research task** *(RT4)* was then formulated as to answer the question: *What State-level strategies are there for reducing the risk posed by botnets and how can we assess their efficiency?*

To achieve this it was firstly necessary to develop a set of potential strategies to choose from. Furthermore, it was necessary to develop a model and to apply an appropriate and well-founded method within it to evaluate the effectiveness of the strategies under consideration.

To develop this set of strategies, it seemed reasonable to take the cyber attacks against Estonia as the motivation and basis for analysing the lessons identified and learned by Estonia. **Publication IV** reflects the findings of this case study.

With the application of data mining techniques, these findings were further extended through a literature review, participation in various international work groups and case studies to finally lead to a framework of strategies to affect the botnet threat.

---

[23] Some of the attacks botnets are commonly capable of performing, namely DDoS, are nearly impossible to defend against (Plohmann, Gerhards-Padilla and Leder 2011). It is especially due to this capability that botnets became the weapon of choice for many different cyber actors from individuals to States, as discussed earlier.

[24] A tactical takedown is a more aggressive effort by the party under a botnet attack to take out the botnet currently attacking rather than limiting oneself to mitigating the negative effect caused by it.

With this framework developed, the DEMATEL method was selected and applied to analyse these strategic options. As part of this method, an **influence model** was developed, linking the various strategies (grouped in strategy groups of similar nature) to the effects of the botnet threat. These effects were either existing shortfalls, missing capabilities in fighting the botnet threat or alternatively existing problems.

The influence model was set up so that if the results of the analysis in a strategic group have an influence with a positive value, this is seen as being appropriate for reducing the threat posed by botnets.

The findings of this analysis were published as **Publication V**, ultimately answering the research question of this dissertation.

II.2 Research Strategy and Main Research Methods Used

The research presented here involves five research papers addressing the four research tasks: each of them selecting and applying different research methods as appropriate to address the respective research task.

Overall following a positivistic research strategy (for the discussion on quallitativ vs. quantitative reserach see e.g. J. Mahoney 2006), case studies combined with system analysis techniques were the main methods used for the research in **Publications I to IV**.

The case study method is regarded as an established way to collect valid and reliable evidence in the research process. *"The case study allows the investigator to concentrate on specific instances in an attempt to identify detailed interactive processes which may be crucial, but which are not transparent to the large-scale survey"* (Remenyi and Money 2006) – and was selected for this very reason.

As a result of the system analysis applied in **Publication II**, a taxonomy was developed. This taxonomy follows the principles of mutual exclusiveness, exhaustiveness and replicability as suggested by Killourhy, Maxion and Tan (2004).

Publication V used a multi-criteria decision-making method called *Decision-Making Trial and Evaluation Laboratory* (DEMATEL), developed between 1972 and 1976 by the Science and Human Affairs Program of the Battelle Memorial Institute of Geneva. *"It can elevate the understanding of the issues, groups of interacted factors, criteria and provide a feasible solution by building a hierarchical relevant network system"* and has been successfully applied to a multitude of different problem settings in different domains (see e.g. the examples provided in Wu 2008; Lin and Tzeng 2009; Chou and Chen 2012; Wen-Shiung Lee et al. 2011). This includes especially its application to evaluate strategy options as in Geers (2011).

The four essential steps of the DEMATEL method are a) to find the average matrix, b) to calculate the normalized initial direct-relation matrix, c) to continuously decrease the indirect effects, and finally d) to set a threshold value and to obtain an impact-relations map. These steps are presented in detail in Li and Tzeng (2009).

As part of this process, informed experts need to be consulted to collect their expert knowledge as the input for the DEMATEL analysis. A small group of 11 recognized international experts was approached with experience in cyber security or botnet matters from industry, government and academia, as well as with a technical, management and legal background. For this task closed-ended questionnaires were used, an established method deemed appropriate, and where necessary additional interviews were conducted to confirm the data collected.

II.3 Research Findings

II.3.1 Results of the First Research Task

Research task 1 was set to answer the question *(RT1): What is the nature of cyber weapons and to what extent does it differ from the established principles of conventional arms and warfare, and further, what are the implications for cyber conflict?*

Before presenting the findings, it is important to provide definitions for two essential terms.

> ***Definition 1: Vulnerability (in IT Systems)***
> *A vulnerability is an exploitable flaw in an IT system, which allows an attacker to usurp privileges or trust, access data or execute commands he normally would not be allowed or expected to. This includes a mis-configuration or known default configuration but excludes social engineering means. Possible examples are: taking control of a system, reading or modifying information stored or processed or adding functionality.* ***(Publication I)***

> ***Definition 2: Cyber Weapon[25] and Cyber Attack.***
> *A cyber weapon is data and knowledge that is capable of, designed to and executed with the intention to affect the integrity, availability and/or confidentiality of an IT system (target) without its owner's approval. The target's defence is overcome by abusing existing vulnerabilities in the target.*
> *The application of a cyber weapon shall be referred to as a Cyber Attack. (**Publication I**)*

[25] In a response to the definition of cyber weapons developed in **Publication I** it was pointed out, that Lorents and Ottis (2010) also present a similar definition of this term. This research still sticks to the one presented here due to the crucial difference, that Lorents and Ottis excluded these means of cyber activities not based on soft- or hardware as not being a cyber weapon. This would mean that cases of "hacking", where no IT system was used, would not be considered cyber weapons. The presented research argues, that if the steps for conducting a successful attack were well documented and repeatable, then such instructions (the knowledge represented by them) are also classified as a cyber weapon.

Cyber aggressors, to achieve their goals, use very different types of cyber attacks as well as related methods and tools. Figure 6 illustrates this by offering a simple yet sufficient classification of cyber weapons (as defined above), also identifying the position of botnets as one of the main types of cyber attacks.

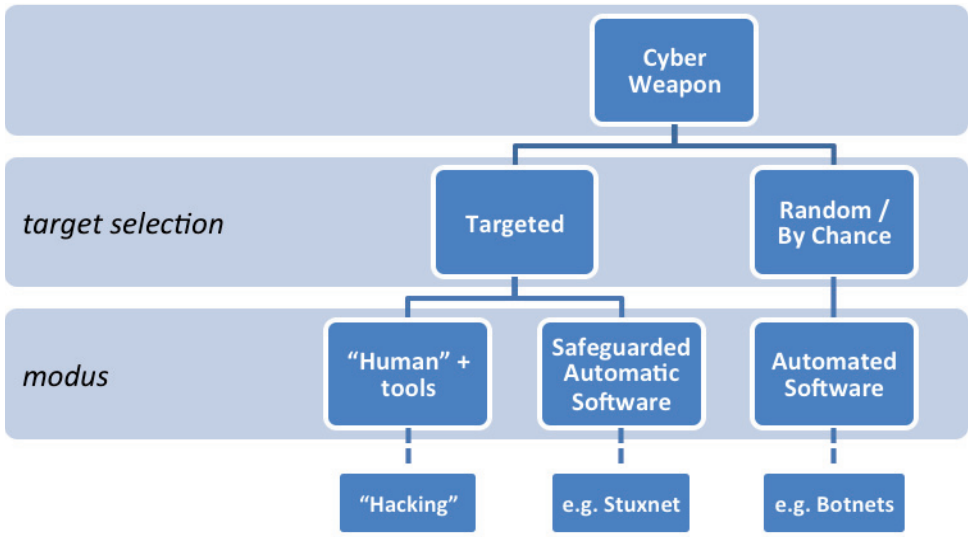

Figure 6. Simple classification of cyber weapons (drawing by the author)

The research concluded that the principles of cyber weapons are sufficiently different from those of conventional weapons to justify them standing on their own grounds. While similarities regarding the conventions of weapon deployment and working principles were found, cyber weapons represent a new combination of these with some essential new features. The key observations are as follows:

1. *The distance between attacker and target is irrelevant* for conducting the attack as long as there is connectivity between them.
2. *Launched attacks hit their target almost instantly.* The defensive aspect of time, which can be used in conventional warfare to start a countermeasure against an attack, becomes less relevant.
3. *There is no border or neutral area.* The notion of national territory or borders has only limited practical meaning on the internet.
4. *Attributing an attack to a specific cyber attacker via technical means is nearly impossible*. If an attacker plots his attacks with enough care, he could even maintain a steady attack on his adversary without being identified.
5. *Cyber weapons do not have a physical nature*[26]. Like ordinary files, these cyber weapons can be copied without noteworthy costs resulting in the

[26] While it is recognized that cyber attacks do have a physical representation e.g. in the form of electrons transported via a wire, they are not essential for the effect caused. Rather it is the knowledge or data coded by them, which – interpreted in the target system – causes the desired effect.

number of copies of a cyber weapon as well as storage or transportation being irrelevant[27].

6. *The costs associated with producing cyber weapons are mainly related to human resources and the* use of inexpensive IT equipment.

(excerpt taken from **Publication I**)

Furthermore, it was discovered that the knowledge of a target's vulnerabilities (as defined above) and how to exploit them is of crucial importance for both the attacker and the defender for their respective interests. This leads to the identification of two important observations:

1. *Cyber weapons are subject to quite a rapid time-decay.* If a cyber weapon is exploiting a vulnerability, it is effective as long as the target IT system has this vulnerability. Vulnerabilities become discovered and patched, and target systems can change their software/hardware at will, so the period of effectiveness for a cyber weapon is undefined, but likely to decrease the longer the vulnerability is known.
2. C*yber weapons usage may lead to the target enhancing its defence* in a very short time. As soon as a cyber attack is executed, the target might have the means in place to detect that an attack occurred and how it was conducted. While the initial attack might have been successful, the likelihood that a proper defence can be built afterwards is reasonably high, rendering the cyber weapon useless against the same target and even against others in cases of existing cooperation or disclosure.

(excerpt from **Publication I**)

Having identified the importance of the knowledge of vulnerabilities, **Publication I** further explored their role from a cyber conflict perspective by developing and presenting a vulnerability-based model of cyber conflicts.

This assumes reasonable actors and vulnerabilities being the central determination for a successful cyber attack. The model can be applied to any set of actors[28] and assumes they are willing and capable of closing all vulnerabilities known to them. As many vulnerabilities are commonly known (and against best practice commonly not fixed in many cases), what are referred to as *0-day vulnerabilities*[29] are of the highest importance giving everyone with knowledge of them an essential advantage. With this, the knowledge of, further discovery of and even exchange of 0-day vulnerabilities becomes of strategic importance. Further discussion of these assumptions is left for **Publication I.**

[27] in size and quantity

[28] may it be it an individual, an organisation, a State, or a mixed set of these

[29] These are vulnerabilities in IT systems which are not yet known and disclosed to general public. By exploiting them by developing and applying a so called 0-day exploit, a particular computer systems can be attacked with a high likelihood of success. "0-day" refers here to the fact that the victim has no time for correcting measures between the discovery and the exploitation of the vulnerability.

Publication I presents this vulnerability-based model of cyber conflicts in more detail and discovers some interesting implications for the relationship between cyber actors. The key findings are summarized as follows.

- Forming *Cyber Coalitions*, in the form of a mutually agreed exchange of vulnerabilities between a limited numbers of actors, in fact results in a collective increase of offensive as well as defensive cyber capability. Furthermore, it is not possible to have one without the other.
  This results in the insight that in the cyber domain no purely defensive *Cooperative Cyber Defence* is possible as soon as knowledge about vulnerabilities is exchanged between partners and not with the public.
- Another surprising observation is that a party following a pacifist attitude could, in the cyber domain, take a proactive stand and actively search and publicly disclose vulnerabilities. Doing so would frequently "destroy" cyber weapons developed by any cyber engaged actor without any real means left for him to prevent this. As such the "pacifist" can actively damage cyber weapon arsenals globally without attacking anyone or causing harm.
- Finally, this model provides an answer to current discussions about how a cyber weapon disarmament procedure could be established (Denning 2001b), as public disclosure of the vulnerabilities used for a particular cyber weapon would render it useless for future usage. Unlike cases of the disarmament of conventional weapons, which affect only the disarmed party, cyber disarmament has a global effect and also affects all other cyber weapons using the same vulnerabilities.
  In this context, the research revealed a paradox that, contrary to conventional weapons, cyber disarmament will not reduce the defensive capability of the disarmed party as it is assumed that this party was protected from its own known vulnerabilities to start with.

After this research task was concluded, a work by Arimatsu (2012) was published also discussing the options and limitations of cyber disarmament. She concludes that cyber arms control is *de facto* impossible for practical reasons. One reason can be seen in the fact that a cyber weapon cannot be easily identified as such, which is a technological limitation. Another is that because of their missing physical form, they are difficult to detect, and therefore, easy to hide (Arimatsu 2012).

While this does not challenge the method proposed for cyber disarmament presented in Publication I, it suggests that this method will never be executed.

II.3.2 Results of the Second Research Task

Research task 2 was set to answer *(RT2): What is the current state of botnets usage?*

To further understand the role botnets play in cyber conflicts, research was conducted to find out what botnets are used for today and by whom. To this end, a usage-centric botnet taxonomy was developed (see **Figure 7**). The detailed descriptions and justifications of each single taxon are presented in **Publication II**.

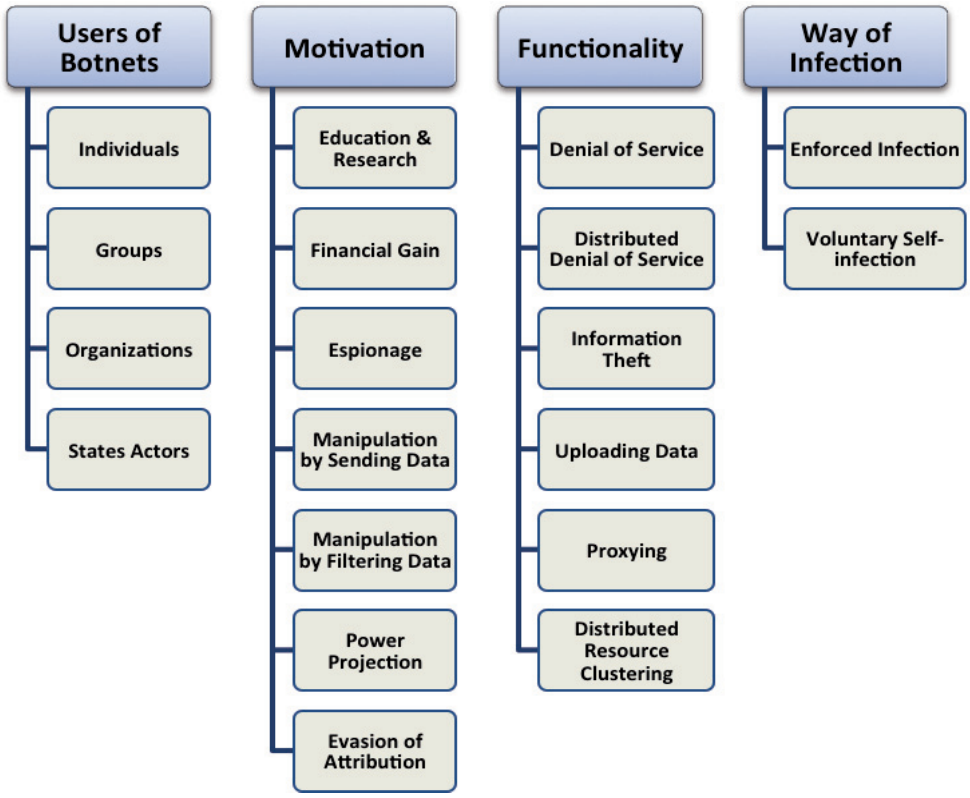

Figure 7. Usage-centric Botnet Taxonomy (**Source: Publication II**)

Following the taxonomy developed, **Publication II** applied its classification to a selection of past incidents to demonstrate its applicability. This is illustrated in Table 1. The full description of the incidents is left for **Publication II**.

Table 1. Selected botnet incidents and their classification according to the developed taxonomy **(**Source: **Publication II)**

Example	**User**	**Motivation**	**Functionality**	**Way of infection**
Stuxnet	State Actor	Power Projection	Denial of Service	Involuntary
GhostNet	Unknown	Espionage	Information theft	Involuntary
Operation Payback	Group	Power projection	DDoS	Voluntary
Israeli	Group	Power Projection	DDoS	Voluntary
Conficker	Group	Education&Research	none	Involuntary
Mariposa	Group	Financial Gain	Information Theft/ DDoS	Involuntary
Belarus Censorship	State Actor	Power Projection	DDoS	Unknown

With regard to the relevant research task, it became evident that botnets are no longer simply a tool for cyber crime related actors seeking financial gain.

While cyber crime is still an important reason, reflected in the well-established and steadily increasing underground economy developing and selling botnet technology and services to everyone willing to pay, increasingly more players are developing and using botnet technology for their own benefit.

This includes States or legitimate companies providing the same technology as organized cyber crime for others including State agencies. In addition, the use of botnets in the context of hacktivism has increased noticeably.

The research further identified the motivations for the use of botnets being (State sponsored) espionage, political (including censorship by States and hacktivism activities) or military operations at different levels of intensity.

II.3.3 Results of the Third Research Task

Research task 3 was set to answer the question *(RT3): What resources (in terms of skills, time and money) are required to set up a botnet compared to those needed to take one down?*

To develop an answer, three broad groups of botnets were defined as: 1) open source botnets, 2) construction kit based botnets, and finally, 3) specialized botnets. A detailed definition of each group is available in Publication III. Some essential attributes of these groups include the following.

The first group encompasses mainly the botnet technology of the first hour, where most parts of the source code are currently publicly available. Later non-public siblings of the original sources are also included.

The second group includes all botnets developed with the main interest in providing a quality product to a wider audience willing to pay for it and the related services. They commonly include license schemes, frequent updates and patches, new functionality, support channels and even infection guarantees. Their development process commonly follows best practices in software engineering and code protection[30].

The last group includes botnets developed with a similar effort and sophistication as the second group but in addition might involve cross domain knowledge and assets beyond ordinary software development like conducting target intelligence. These botnets are often developed for a particular purpose, using the highest level of sophistication to achieve it. This purpose might not be of monetary nature at all, and the developers of these botnets are often not interested in the later sale of their creation.

The findings of **Publication III** with respect to the skills, money and time needed to develop, obtain, deploy, maintain and take down these different groups of botnets is summarized in Table 2. Some key findings are elaborated in the following, leaving further details for **Publication III**.

[30] This is among others achieved using software code protection techniques like code obfuscation, binary compression or debugger traps, but also encryption or licence enforcement.

Table 2. Summary of requirements for setting up and taking down botnets (Source: the author)

	Group 1	Group 2	Gruop 3
Develop	*Easy to moderate* *Most code base already developed and available for free; community support often available*	*Complex* *highly skilled developers in different disciplines needed*	*Complex* *highly skilled developers in different disciplines needed; access to further domain knowledge or intelligence often required*
Obtain	*Easy* *often free of charge*	*Easy* *Sold through criminal channels for a few thousand USD*	*Difficult and expensive, often self-developed by specialists*
Deploy	*Easy*	*Easy*	*Easy to moderate*
Maintain	*Easy*	*Easy*	*Easy to moderate*
Takedown	*Moderate combination of different skills required; the availability of the source code facilitates the efforts needed*	*Moderate to complex combination of different skills required; the availability of a botnet-kit reduces the efforts slightly; often involvement of multiple authorities and/or service providers necessary*	*Complex* *combination of different skills (sometimes in different domains) required; often involvement of multiple authorities and/or service providers necessary*

It was concluded that acquiring and deploying a botnet is a rather easy endeavour for botnets in the first two groups. These botnets can be purchased as a service for a few hundred dollars per day or acquired for a few thousand USD or found for free.

The configuration and deployment often requires average computer skills as these botnets are developed with user-friendliness in mind. Still, the owner of a botnet needs to have a proper knowledge of securing his C&C server infrastructure, which is independent from the botnet technology used, but still essential for its overall success. These botnets suit most cases resulting in a low threshold for acquiring and deploying botnet technology.

The same is true for specialized botnets with the exception that acquisition is a difficult task. Their specialized nature dramatically limits the availability of appropriate technology, and the special (security) requirements dictate that these botnets need to be developed by the user himself.

With regard to the resources necessary for developing a decent botnet, **Publication III** identifies this as the most complex and challenging part in the life cycle of botnets. The development efforts scale directly with the desired level of resistance towards detection and takedown as well as the level of the sophistication of the functionality provided. Highly skilled teams of experts are commonly required for this.

The requirements further increase for specialized botnets in terms of their need to reach a very specific objective or to perform a very specific function for the best possible outcome.

The last aspect covered by **Publication III** was to discuss the efforts needed for a tactical botnet takedown, which means to conduct countermeasures against the originating botnet rather than relying on common defensive techniques. The effectiveness of the latter is commonly regarded as limited, especially in the case of botnets being used for DDoS attacks, as common defensive techniques such as firewalls, IDS or antivirus solutions primarily only act on the local level (Leder, Werner and Martini 2009). A selection of the most common tactical countermeasures is introduced in more detail in **Publication II**. Estimates of the skill and time needed for these are summarized in Table 3.

Table 3. Time and effort estimates for common tactical botnet countermeasures (Source: the author)

	Skills & Activities needed	**Response Time Estimate**	**Remarks**
C&C Server Takedown	Medium - mainly network intelligence needed to determine IP addresses of involved entities	- Few hours to days for detection, - multiple days to weeks for international cooperation, - quick execution	Requires support from hosts and often local authorities
DNS-based Countermeasures	Low - mainly coordination activity with DNS registrars	- Few hours to days for detection, - multiple days to weeks for international cooperation, - countermeasure takes effect latest within a few days	Requires the cooperation of DNS registrars and often local authorities
Response DDoS	Very low - an automatic system is easily set up and can be launched by anyone	- Few hours to days for detection, - counter DDoS immediate	Only suppression of C&C servers

Hack-Back	High - Hacking skills - network intelligence skills - Reverse engineering skills	- Days to weeks	Further intelligence on the botnet owner possible
Infiltration	High - Hacking skills - network intelligence skills - Reverse engineering skills	- Several weeks	Complete control: Take-over or clean up possible
BGP Blackholing	Low - mainly coordination activity with ISP	- Few hours to days for detection, - Black hole established within minutes	

A tactical takedown often requires time consuming reconnaissance and analysis to be conducted before a sustainable takedown can be achieved. Furthermore, most countermeasures require the support of Internet Service Providers or DNS registrars on a global scale and with this cooperation between law enforcement authorities of multiple States to be successful and sustainable.

In the course of the research conducted it also became evident that many of these aggressive counter measures use techniques commonly regarded as illegal; even if executed in good faith.

In summary, **Publication III** showed that setting up or acquiring a botnet is a rather simple task, which literally everyone is capable of, assuming enough motivation and funds are available. Developing botnets on the other side is a highly challenging endeavour reflected in the well-established organized cyber crime landscape of malicious software programming service providers.

A botnet takedown is a difficult and time consuming activity on the technical level. The international distribution of botnets requires either the use of illegal techniques (even if conducted in good faith) or relies on generally time consuming, coordinated takedown operations requiring international cooperation.

This brings us to the conclusion that in most cases a tactical timely takedown close to the time of the first attack against a target is not possible.

II.3.4 Results of the Fourth Research Task

Research task 4 was set to answer the questions *(RT4): What State-level strategies are there for reducing the risk posed by botnets and how can we assess their efficiency?*

The first step in dealing with this research task is to develop a set of State-level strategies to enhance a State's cyber security framework and with this its resilience towards botnet mounted attacks.

The case study conducted in **Publication IV** on the changes in Estonia after the cyber attack in 2007 provided the corner stones by identifying five key lessons learned, which can be considered a strategic approach. They are:

1. Developing or enhancing the State's national cyber security framework.
2. The implementation of the Council of Europe Convention on Cybercrime.
3. Cyber security awareness and education in society in general.
4. Active participation in international cooperation efforts.
5. Engage in public-private partnership programs and harvest the potential of volunteers for national security efforts.

Development of a Framework of Strategy Options

These findings and subsequent research resulted in the formulation of 10 groups of State-level strategies, each of them encompassing strategies of a similar nature. They are introduced in detail and discussed in **Publication V**. The following serves as a brief summary (excerpt from **Publication V**):

1. *Promotion of dedicated and coordinated R&D Programmes*
   This group covers strategies such as the development or promotion of nation-state research agendas, the support of these with special grants or programmes, or the development of new/specialized curricula.

2. *Improvement of international law enforcement*
   This group reflects efforts such as the Council of Europe Cybercrime Convention aimed at the harmonization of criminal code for cyber offenses. Agreements between nation-states, legislation or regulations within supranational organizations such as the EU, or commitments of or recommendations to nations under the umbrella of international organizations are other possibilities.

3. *End-user notification, support and good-behaviour incentives*
   This group firstly covers activities aimed at establishing a system for notifying end-users about a current infection, and to help them in the process of clearing the infection from their systems. Secondly, governmental and

successively ISP[31]-based instruments to encourage good behaviour are included.

4. *ISP obligations and incentives to act*
   This group of strategies reflects actions to encourage ISPs to implement means and processes to pre-emptively mitigate botnet infections or their actions. There are various mechanisms for these, ranging from financial support or loans to active negotiations or regulations enforced by ISPs.

5. *Awareness campaigns*
   This group encompasses measures taken to raise general public awareness on a broad and continuous basis, similar to campaigns for AIDS, smoking or drugs.

6. *Development of over-arching State cyber security strategies*
   This group reflects the process of developing and implementing a dedicated State-level cyber security strategy or policy, and the subsequent reorganization of State responsibilities and authorities.

7. *Promotion and support of botnet hunting initiatives*
   This group encompasses active efforts of States to encourage, facilitate and perhaps even financially support botnet hunting initiatives emerging from the private sector or academia.

8. *Software developers' obligations or incentives*
   This group includes efforts to increase the pressure on software developers to produce more secure (proven) code. There are a variety of instruments available, starting with the promotion and subsequent requirement of certified compliance with standards in public procurement or the obligation to clearly indicate compliance to customers. Another method is the introduction of liability obligations for software developers or a mandate/ incentive for software developers to release security patches to all users, including those using illegal copies.

9. *Obligation of cyber insurance*
   This group reflects the encouragement of cyber insurance and the possible introduction of the obligation to be insured. This obligation could especially be aimed at key industries that are identified as critical by a State.

10. *National or international partnership programmes and information exchange*
    This group represents the active promotion of, participation in and contribution to national and international partnership programmes between the public and private sector.

[31] Internet Service Providers

DEMATEL Evaluation of the Framework of Strategy Options

To satisfy the chosen evaluation method, a framework of effects on the botnet threat by these strategies was defined as follows:

I. (Improving) Detection, monitoring and tracking of Botnets
II. (Reducing the) existing botnet population
III. (Reducing the risk of) new infections and migration to new victim platforms
IV. (Reducing profitability of the) cyber crime economy behind Botnets
V. (Reducing/deterring) botnet usage by APT or State-sponsored Espionage/CNO
VI. (Reducing/deterring) botnet usage by Hacktivism
VII. (Inhibiting the) development and proliferation of botnet technology

Matrix 1. Input matrix for DEMATEL analysis. (Source: Publication V)

	S1 R&D Programs	S2 Intern. law enforcement	S3 End User	S4 ISP obligations & incentives	S5 Awareness campaigns	S6 Cyber security strategies	S7 Botnet Hunting	S8 SW Developers' obligations	S9 Cyber Insurances	S10 Partnership programmes	E1 Detection of Botnets	E2 existing population	E3 new infections	E4 Cyber Crime Economy	E5 APT/state-sponsored usage	E6 Hacktivism botnet usage	E7 Technology proliferation	Total Influence
S1	0,0	0,4	0,9	0,8	1,3	1,5	2,0	0,8	0,5	2,0	2,3	1,4	1,0	0,5	0,4	0,5	0,7	17
S2	0,5	0,0	0,7	1,9	1,0	1,5	1,3	0,5	0,7	2,0	1,2	1,3	0,8	1,9	0,5	1,5	0,4	18
S3	0,5	0,7	0,0	1,9	2,5	1,3	1,0	0,7	0,9	1,6	1,3	2,1	1,3	1,2	0,2	0,6	0,5	18
S4	1,0	1,3	2,5	0,0	2,4	1,6	1,4	0,7	1,4	2,0	2,7	2,3	1,8	1,5	0,6	1,0	1,2	25
S5	0,8	0,7	2,2	0,8	0,0	1,3	1,2	0,5	0,6	0,6	0,6	1,4	1,5	0,9	0,1	0,4	0,3	14
S6	2,4	2,1	1,0	1,3	1,9	0,0	1,3	0,9	0,6	2,3	1,3	1,0	0,6	0,8	0,7	0,9	0,5	20
S7	2,1	1,6	0,9	1,3	1,1	1,1	0,0	0,3	0,2	1,9	2,9	2,0	1,0	1,4	0,8	0,9	1,2	21
S8	1,5	0,2	0,8	0,6	0,9	0,4	0,3	0,0	1,1	0,8	0,4	1,3	1,7	0,6	0,5	0,4	0,8	12
S9	0,9	0,4	1,4	1,3	1,2	0,8	0,6	1,2	0,0	0,6	1,0	0,7	0,7	0,4	0,2	0,4	0,2	12
S10	1,6	1,9	1,6	1,2	1,2	1,5	1,5	0,4	0,2	0,0	2,0	1,3	1,1	0,6	0,5	0,4	0,5	18
E1	1,6	1,5	1,1	1,1	0,8	0,7	2,1	0,2	0,3	2,1	0,0	1,8	1,1	1,2	0,6	0,9	0,8	18
E2	1,0	1,2	0,9	0,8	1,3	0,7	1,7	0,4	0,3	1,6	2,1	0,0	1,8	1,9	0,8	1,3	1,0	19
E3	1,2	0,3	0,7	0,6	1,0	0,8	0,9	0,4	0,2	1,0	1,6	1,9	0,0	1,4	0,6	0,6	1,1	14
E4	0,6	1,3	0,3	0,4	0,4	0,9	1,0	0,2	0,2	1,3	1,4	2,2	1,5	0,0	0,1	0,1	1,3	13
E5	0,9	1,0	0,1	0,3	0,3	1,8	0,7	0,1	0,2	0,9	0,7	0,5	0,7	0,4	0,0	0,6	0,4	10
E6	0,5	1,2	0,4	0,6	0,8	0,8	0,6	0,1	0,1	0,7	0,5	0,6	0,3	0,3	0,4	0,0	0,3	8
E7	0,9	0,5	0,6	0,7	0,4	0,7	1,2	0,7	0,1	1,1	1,6	1,8	2,0	1,0	0,6	0,5	0,0	14
Level influenced	18	16	16	16	19	17	19	8	8	23	24	24	19	16	8	11	11	

As a result of the collection of empirical data, Matrix 1 was compiled and served as an input for the subsequent calculations prescribed by the DEMATEL method. With regard to the Strategy Option, the results are illustrated in terms of the influence map presented in Figure 8.

The net influence, plotted on the y-axis, is the difference between received and introduced influence in the system and is a measure of the contribution to the system, meaning the reduction of the botnet threat.

The total influence, plotted on the x-axis, is the sum of the received and introduced influence and is a measure of the interconnectedness of an element in the system. The higher this value, the more the particular strategy intervened.

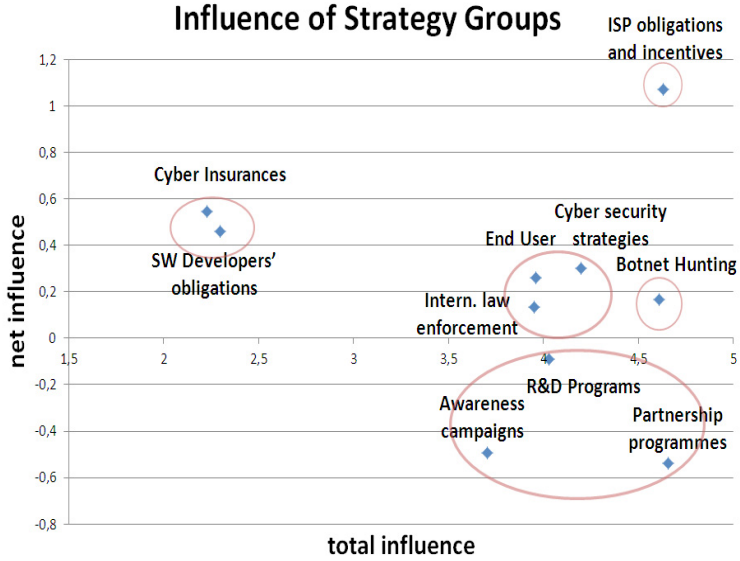

Figure 8. Influence Map of Strategy Groups (Source: the author)

As can easily been seen in the influence map, the analysis strongly supports the common belief that focusing on *ISP Obligations & Incentives* in the fight against botnets is the most promising strategy.

What is surprising is that the strategy groups *Cyber Insurances* and *Software Developers' Obligations* rank second with about 50% less net influence than the most influential strategy group. On the other hand, they show the lowest total influence reflecting the fact that they are commonly not regarded as an important or feasible strategy to invest in. The findings of this analysis provide reason to challenge this general understanding and to recommend more attention be given to these strategies.

A similar conclusion can be made in the case of *Botnet Hunting* initiatives; while there has been some activity in this area already, as discussed in **Publication V**, there is no broad State support for these initiatives. The analysis shows a very high total influence value (while still having a positive net effect) reflecting this strategy's high interconnection with other strategies.

The strategy groups *Cyber Security Strategies, End-user Obligations* and *Intern. Law Enforcement* form a cluster with a moderate net influence on the problem, and a decent level of interconnectedness making them all good candidates.

The last cluster consists of the strategy groups focusing on *Partnership Programmes*, *R&D Programmes* and *Awareness Campaigns*. While all of them are highly interconnected with other elements in the system, they are all net recipients (with the exception of R&D programmes which has close to zero net influence). They do not contribute to the fight against botnets, but draw influence away, making them the least attractive strategy to invest in.

Applying a similar (short) net influence analysis on the seven effects on the botnet threat revealed that all of them **beside** *State-use of Botnets* and *Botnet Technology Proliferation* are affected so that the threat is reduced. The actual ranking is presented in Table 4.

An explanation for the steady increase in botnet technology proliferation can be two-fold. Firstly, as discussed earlier in this dissertation, increasingly new actors are becoming engaged in malicious cyber activities. With this the demand for botnets is increasing. Secondly, one essential part in the botnet takedown business is the development of new means and methods, provoking the botnet industry to develop appropriate countermeasures leading to new products looking for customers.

Table 4. Remaining influence on the botnet threat (Source: Publication V)

Effect on Botnet Threat	**Net Influence**
E1 Detection of botnets	-0,66
E2 Existing population	-0,58
E3 New infections	-0,49
E4 Cyber Crime Economy	-0,34
E6 Hacktivism botnet usage	-0,32
E5 APT/State-sponsored usage	0,23
E7 Technology proliferation	0,34

The fact that the State use of botnets is not well influenced (in contrast to the other two main actor groups in this analysis being hacktivists and criminals) is more difficult to explain. The most plausible reason might be the fact that State actors or APT agents are to a lesser extent dependant on the underground market, as it is assumed they have the capabilities to develop the necessary technology themselves. Further, concerning their persistent nature, they are less deterred by countermeasures or the risk of facing law enforcement actions.

Prioritization and Recommendation of Strategy Groups

Based on the findings presented so far and under the assumptions made and explained earlier, this research argues in favour the priority of *ISP Obligations and Incentives* as the most promising strategy to follow.
As a second priority, more attention should be given to *Cyber Insurance, Software Developers' Obligations* and *Botnet Hunting* initiatives, as they are commonly believed to be more influential.

As a third priority, States should continue or increase their focus on actions concerned with developing *Cyber Security Strategies* geared towards *End-user Obligations and Good-behaviour Incentives* or leading to more *International Law Enforcement Agreements.*

States are discouraged from investing too much in *Partnership Programmes, Awareness Campaigns* or *R&D Programmes,* with the latter being a borderline call.

PART III. PUBLICATIONS

PUBLICATION I: A VULNERABILITY-BASED MODEL OF CYBER WEAPONS AND ITS IMPLICATIONS FOR CYBER CONFLICT

Christian Czosseck and Karlis Podins

Proceedings of the 11th European Conference on Information Warfare and Security,
Laval, France 7-8 July 2012, pp. 198-205.

ISBN: 978-1-908272-55-3

Abstract: Throughout history, mankind has developed and employed novel weapons systems and equally novel countermeasures. Naturally, both offensive and defensive systems are limited by the laws of nature. Consequently, military concepts and doctrines were designed by implicitly taking into account those same limitations. The digital age has introduced a new class of weaponry that poses an initial challenge to our common understanding of conflict and warfare as for their different characteristics: cyber weapons. Cyber weapons and other terms like hacking are used frequently, commonly without giving clear definitions in the given context. We propose a restricted definition of cyber weapons as consisting primarily of data and knowledge, presenting themselves in the form of prepared and executed computer codes on or a sequence of user interactions with a vulnerable system. This article explores the crucial differences between the conventional weapons and cyber weapons domains, starting a debate on to which extent classical concepts and doctrines are applicable to cyber space and cyber conflict. This motivates a discussion on the role of vulnerabilities in IT systems, and their impact to IT security and cyber attacks. The authors describe a vulnerability-based model for cyber weapons and for cyber defense. This model is then applied to describe the relationship between cyber-capable actors (e.g. nation-states). The proposed model clarifies important implications for cyber coalition-building, and disarmament. Furthermore, it presents a general solution for the problem of the destruction of cyber weapons, i.e. in the context of cyber arms control.

Keywords: cyber weapons, cyber defense, disarmament, coalition, vulnerabilities

1. Introduction

As conflicts have moved into cyberspace (and vice versa), a clear understanding of cyber weapon becomes a necessity. The development of weapons was always part of mankind's history. Weapons evolved to suit the tactics, but from time to time new weapons revolutionized the tactics and strategies of warfare. The developments of artillery, gunpowder, aviation or weapons of mass destruction are just some examples from recent history. They all caused dramatic changes on the face of the battlefield. But all those weapons developed so far have similar kinetic and/or thermal properties due to the shared physical domain.

In the cyber attacks on Estonia in 2007, a campaign of massive distributed denial of service (DDoS) attacks against government websites, paired with hacking attempts against valuable targets like ISP backbone routers, a new type of conflict

became a reality (Evron, 2008). Many more politically motivated DDoS attacks followed (Nazario, 2009). It drew strong and inconsistent media attention, up to being termed the first cyber war in history, as discussed by (Farivar, 2009). While Article 5 of the North Atlantic Treaty, governing mutual support among NATO nations in case of an armed attack was not invoked, national security leadership around the world received a wakeup call. However, several years later we still have not seen a commonly agreed definition of cyber weapons or cyber warfare (Ottis & Lorents, 2010).

In first section we are going to define basic terms and give short overview about special properties of cyber domain and cyber weapons. The concepts and terminology initially used were based on our understanding of conventional weapons or weapons of mass destruction (Sharma, 2009). Unfortunately, cyber weapons, being data and knowledge, follow other rules than their conventional counterparts. Thus the effects of cyber weapons on their target are different. In 2007 a direct, destructive cyber attack on a power generator was proven possible in a real life experiment (Herold, 2007). Latest prominent case, the Stuxnet virus, which is assumed to have sabotaged the Iran nuclear program starting from 2009, shows how powerful a cyber weapon in a real world setting can be (Falliere, Murchu, & Chien, 2010; Langner, 2011). Some research states that conventional weapons framework is ineffective, is not applicable or has left a big gap between our assumptions about cyber weapons and reality (Sulek & Moran, 2009). We do not want to get involved in this controversial discussion, but rather explicitly show some surprising aspects of cyber domain.

Section 2 of the paper introduces a vulnerability-based model of cyber conflict. We argue that knowledge about vulnerabilities is key and atomic element in both cyber offense and cyber defense, and build a simplified model of cyber conflict around this idea.

In section 3 we will apply the vulnerability-based model on selected aspects of cyber conflicts. By using the proposed model to describe relationship and interactions between cyber-capable actors we demonstrate applications of proposed approach.

2. The Cyber Domain and its Weapons

In recent years, the prefix CYBER has become quite common and was added to many existing terms with the intention of extending its meaning into cyberspace (Ottis & Lorents, 2010). While terms like cyber war (warfare), cyber defense or cyber weapons are widely used, there is a lack of commonly accepted definition, and authors often use terms without precisely describing their meaning.

In the context of this paper we would like to offer the following definitions.

Definition 1: Cyber Weapon and Cyber Attack.
A cyber weapon is data and knowledge that is capable of, designed to and executed with the intention to affect the integrity, availability and/or confidentiality of an IT system (target) without its owner's approval. The target's defense is overcome by abusing existing vulnerabilities in the target. Application of cyber weapon shall be named a Cyber Attack.

Definition 2: Vulnerability.
A vulnerability is an exploitable flaw in an IT system, which allows an attacker to usurp privileges or trust, access data or execute commands, he normally would not be allowed or expected to. This includes mis- or known default configuration but excludes social engineering means. Possible examples are: taking control of a system, reading or modifying information stored or processed or adding functionality.

When starting discussions on conflicts in cyberspace, one should clearly understand the cyber domain and its special properties. Cyberspace differs from conventional weapons domains, some differences being minor while some are of the utmost importance. We believe that ignoring these differences and straight-forward application of established concepts especially on weapons has caused some of the confusion around the cyber domain. In the following an overview of key differences between the cyber domain and the domain of conventional arms is provided. As for space reasons, an analogy to the domains of nuclear, biological and chemical (NBC) weapons is not made.

The confusion can be easily explained just by looking at the definitions. While established concept assumes weapon to be a physical object, cyber weapon under proposed definition is knowledge and data derived from it.

The extent and severity of cyber attacks can vary as recent history has shown, from local (loss of email confidentiality due to loss of password) to nation-wide (Ottis, 2008). As for the time being, *cyber attacks do not directly kill* living beings, but can cause abuse of, malfunctions or the destruction of equipment. That, as a 2nd or higher order result, can lead to a lethal effect or further destruction (Ziolkowski, 2010).

The distance between attacker and target is irrelevant for conducting the attack as long as there is connectivity between them. By connectivity we mean possibility to communicate between the attacker and the target, including not only wired or wireless media, but also methods to transfer information between air-gapped networks (see e.g. Falliere et al., 2010; Langner, 2011). Considering the Internet as the global network, all connected computers, smart phones, cars, industrial control systems (SCADA), or Internet enabled household electronics are just some of the possible targets. As of the very nature of the Internet a cyber attack can be initiated from any (connected) place on this planet to reach almost everywhere.

Launched attacks hit their target nearly instantly. While preparing a cyber attack might demand time consuming preparations, some of the effects could manifest itself in the blink of an eye. With this the defensive aspect of time, which can be used in conventional warfare to start a countermeasure against an attack, becomes less relevant.

There is no border or neutral area. National territory or borders on the Internet are only considered by legal departments, e.g. (Kelsey, 2008), but so far those concepts have almost no everyday practical meaning. While it is possible to cut or limit nation's connectivity to Internet, the consequences for any modern nation state are too bizarre to consider it a long term solution.

The attribution of an attack to a cyber attacker is, with technical means, nearly impossible (Hunker & Hutchinson, 2008). While attribution might be possible by also considering information from other sources and by analyzing the behavior and beneficial outcome for other parties (Ottis, 2008), this is not guaranteed. The Conficker worm so far has not been attributed to any party, although considerable public and security community attention was focused to it, as well as USD 250,000 bounty was offered by Microsoft (Microsoft Collaborates With Industry to Disrupt Conficker Worm,?2009). If an attacker plots his attacks with enough care, he could even maintain a steady attack on his adversary without being identified (Lemay, Fernandeza, & Knight, 2010). But having, to a reasonable extent, a confirmed source is a common requirement for the attacked party to take active countermeasures, especially if they are of violent nature (Ziolkowski, 2010).

Cyber weapons do not have a physical nature, they are knowledge and data as defined above. To conduct a cyber attack, the attacker has to send data to the victim. Most can be made persistent, e.g. by writing a script or program and storing this on an IT system. Like ordinary files, those cyber weapons can then be copied without noteworthy costs so the number of copies of a cyber weapon is usually irrelevant. Storage and transportation of cyber weapons also seem easier than for physical counterparts, one party could even decide to keep a copy or even the whole cyber weapon arsenal outside its own borders, hiding it in different places all over the Internet.

Cyber weapons production costs are mainly human resources related. While we recognize the initial investment in R&D as necessary, success of lone hackers and loose groups (Anonymous, LulzSec) shows that a lot can be achieved with limited funds. We believe that especially for a nation-state it is a minor expense compared to development of advanced conventional weapons. The production of conventional weapons depends mostly on the costs of fabrication, which often is a combination of labor costs, materials, machines and infrastructure. In contradiction to this, cyber weapons are constructed mainly by human knowledge on relatively cheap IT equipment. Their skills and knowledge in areas like software development, exploit development and penetration testing are the essence of the attack. Hiring the right

personnel and keeping or extending their skills is the major investment needed to maintain or extend a cyber weapons arsenal (Miller, 2010).

The knowledge of a target's vulnerabilities and how to exploit them is of central importance to the attacker. On the other side, this knowledge is also the most important piece of information needed by the target of the attack to set up an efficient defense.

This leads us to the 1st paradox of cyber weapons: they are subject to time-decay. If a cyber weapon is exploiting a vulnerability, it is effective as long as the target IT system has this vulnerability. Vulnerabilities get discovered and patched, and target systems can change their software/hardware at their will, so the period of effectiveness for a cyber weapon is undefined, but likely to decrease the longer the vulnerability is known. This aspect is also discussed in (Moore, Friedman, & Procaccia, 2010).

The *2nd paradox is that of cyber weapons usage may lead to the target enhancing its defense* in a very short time. As soon as a cyber attack is executed, the target might have means in place to detect that an attack occurred and how it was conducted. While the initial attack might have been successful, the likelihood that a proper defense can be built after it is reasonably high, rendering the used cyber weapon useless against the same target and even against others in cases of existing cooperation or disclosure. An example is specially crafted malware. As soon as samples of a particular new malware get collected and analyzed, appropriate antivirus, IDS and software patching could be done rather fast. Still this is ultimately decided by the capabilities for the actors.

This has consequences for one's ability to test the effectiveness of cyber weapons. As soon as a certain cyber weapon is tested in the wild or even against the target itself, the likelihood is reasonably high to believe that security-aware targets will find a way to enhance their defense against the attack. (It is recognized that techniques are available to the attacker to re-launch the same attack using changed code, and that the target can only learn from an attack if he recognizes it in the first place.) But testing those attacks in a closed test environment will not always guarantee their successful later deployment, as it will be hard for the attacker to build a reasonably complete testing environment with the true attributes of the real target. Nevertheless, it has to be pointed out, that it is quite common to use commercial off-the-shelf hardware and software, which can also be easily acquired by the attacker in order to test his defenses.

The given unique attributes and examples support our opinion, that conventional arms and the ways we use them, are different from cyber weapons. This is why in the following section we propose a model to describe cyber domain and conflicts within.

3. A Vulnerability Based View on Cyber Weapons

The actors (parties) of cyber incidents might be individuals, groups of individuals, companies or nation-states. All possible combinations of parties attacking each other with cyber weapons reflect different scenarios, which, depending on effects, we would call criminal acts, industrial espionage, terrorism, conflicts or even (cyber) war. While a discussion on mapping these terms in the cyber landscape might be reasonable, we would like to state that the proposed model is generic enough to be applicable to all of them, because it focuses on the underlying mechanics. Considering the scope of this paper, we will use the term cyber conflict for all those mentioned combinations.

3.1 Vulnerabilities

Vulnerabilities, the knowledge about and the skills to exploit them, are of utter importance in any form of cyber conflict. It is quite clear that without exploitable vulnerabilities, cyber attacks would be pretty much limited to (D)DoS attacks (as they do not rely on a flaw in the target, but limit their targets' accessibility by exhausting bandwidth, CPU or other limited resource) or attempts to manipulate users through social engineering to get access to the target's system. To reflect that, we propose to take vulnerability as an atomic entity and analyze cyber weapons and conflict by looking at them from a vulnerability point of view.

Vulnerabilities differ in their severity. Some of them enable an adversary to conduct a cyber attack against a target (e.g. root access), while some are likely not to be of any use to an attacker. The internationally recognized Common Vulnerability Scoring System introduces an open framework enabling one to score and compare the severity of a vulnerability based on its intrinsic qualities, its behavior over time and its environmental uniqueness (Mell, Scarfone, & Romanosky, 2007). While comparing individual vulnerabilities, it makes a difference how severe every single one of them is. However, we will save a detailed examination of this issue for future research. For the moment, it might be safe to only consider those potentially leading to a complete violation of availability, confidentiality or integrity of an attacked IT system.

The dynamic nature of IT implies that the set of vulnerabilities changes over time. When new code gets installed, new vulnerabilities are added and/or other vulnerabilities get removed. There is a considerable amount of vulnerabilities publicly disclosed every day (e.g. at the National Vulnerability Database (Security, 2010)) but some vulnerabilities remain unpatched although known to the public for decades (Oiaga, 2010).

Naturally, there exists a set of all vulnerabilities that are in the software installed somewhere. This is not constant and changes every time new software is installed,

removed or configured. Each party has knowledge about some of the vulnerabilities. There are vulnerabilities unknown to all parties. As such the union of all parties known vulnerabilities still might not give all existing vulnerabilities.

3.2 Cyber Defense

Apparently a system without vulnerabilities is well defended against majority of cyber attack (apart from DoS based attacks). The defender of a target system has three options to render a vulnerability-based cyber weapon *w* useless.

- By knowing about vulnerabilities exploited by *w* and having own infrastructure immune against w by patching its own systems accordingly;
- By putting in place means to effectively make an existing, unpatched vulnerability not exposed to the attacker (e.g. by using firewalls hiding a service to the Internet or signature-based attack detection). This would also apply to vulnerabilities unknown to the defender but coincidently covered;
- By putting in place means to detect and mitigate cyber attacks before their effect manifests itself.

One could assume that cyber security aware parties have full control over and knowledge about their own IT assets, making sure not to be vulnerable to attacks they known by themselves (as they ultimately relay on vulnerabilities). Realty shows us that this does not hold true all the time, but nevertheless we keep this assumption for the sake of simplicity, assuming the target to be capable and willing for defending his cyber frontline.

3.3 Cyber Weapons Development

Cyber Weapons are produced based on knowledge of target‘s vulnerabilities. It should be clear that before developing any weapon *w*, a party must have knowledge about the vulnerabilities the weapon will exploit and for any given weapon *w* it is possible to find respective vulnerabilities.

More formally speaking, there exists a natural mapping *e* from cyber weapons to vulnerabilities they exploit. For any given weapon *w*, the set *e(w)* is either empty (in the case of a DoS attack or cases of social engineering) or it contains at least one vulnerability.

Sometimes, successfully attacked IT Systems can be used for manual or automated creation of (new) cyber weapons for further attacks, e.g. sending infected emails to all persons in contact list or probing the local network for other vulnerable machines.

To effectively enlarge one's weapons arsenal with new weapons, a party is required to find an additional vulnerability.

As time passes, other parties discover vulnerabilities in a non-deterministic manner. When a party discovers a vulnerability v, we can assume that their defenses are upgraded, making weapons exploiting vulnerability v ineffective against party p. Research by Moore et al. (Moore et al., 2010) propose a similar vulnerability-based look but assumes the opposite, that own infrastructure is not patched not to warn the opposing parties of discovered vulnerabilities, coming to noteworthy conclusions.

Additionally, it seems reasonable to assume that the target party *t* has adequate logging and attack detection systems in place and will be capable of identifying exploited vulnerabilities at least after they have been used by a cyber weapon, leading to improved cyber defense.
This stresses again the overlap between cyber attacks and defenses and vulnerability discovery plays a central role both for attackers and defenders.

4. Implications on Party Relationships

In following section we will test vulnerability-based thinking by applying it to model cyber disarmament, coalitions, collective defense, pacifism and arms control.

4.1 Cyber Disarmament

In contrast to vague cyber disarmament discussion (Gjelten, 2010) the proposed model offers an effective method of cyber weapon disarmament, as asked for by (Cahill & Rozinov, 2003). Disarmament of cyberspace could be achieved by public vulnerability disclosure. If a party wants to verifiably dismantle some of its cyber weapons, it could publicly disclose all the vulnerabilities used by them. Unlike in real-world disarmament, which affects only the disarming party, cyber disarmament is global. After other parties have adequately reacted to disclosed information, all cyber weapons using disclosed vulnerabilities are rendered useless. This is regardless if they are in the possession of the disarming party or by another party.

But there are further peculiarities. Unlike in the conventional weapons domain, if a party *p* dismantles a set of cyber weapons by disclosing the respective vulnerabilities, defense of *p* is not affected. Following our assumption that a party always tries to be protected against all known vulnerabilities, *p* does not disclose a new attack vector against itself, leaving its adversaries without an advantage by this action.

P's offensive capabilities are decreased by an unknown factor, depending on how many other parties had the disclosed vulnerabilities in their IT systems.

4.2 Cyber Coalitions

If two or more parties would mutually agree on cyber disarmament, public vulnerability disclosure can be used with the consequences as described before. But an interesting approach would be a mutual vulnerability disclosure; it effectively means that cyber weapons involved in the mutual disarmament would be ineffective against other parties involved in the disarmament agreement, but still potentially effective against 3rd parties.

By exchanging information on vulnerabilities between each other one enables the other to build new weapons based on the newly learned vulnerabilities. But at the same moment both become immune to cyber attacks based on the exchanged vulnerabilities, as soon as they have implemented the necessary changes in their defense. Their offensive capabilities to attack each other decreases or remains the same.

Let *c* be any other 3rd party not part of the treaty or coalition between *a* and *b*. With the newly won knowledge both parties *a* and *b* might have gain additional knowledge to build a cyber weapon *c* is vulnerable to, enhancing their offensive capabilities against *c* or at least remaining the same.

4.3 Cooperative Cyber Defense

Based on the definition of cyber defense given above, cooperation in cyber defense between two or more parties can manifest by exchanging of vulnerability information and/or attack detection procedures, if it provides tangible benefits to each party.

But in the case of vulnerability information exchange, there is no difference from the aforementioned cyber coalition. This leads to the observation that it is possible for cooperative cyber defense to be indistinguishable from a cyber coalition.

To arrange a cooperative cyber defense that is purely defensive in nature, the cooperation between the parties would be limited to the exchange of signatures and other attack detection information without sharing vulnerabilities per se. If knowledge about vulnerabilities shall also be shared without giving an offensive advantage to the parties, it must be done by public disclose with the consequences as described under cyber disarmament.

4.4 Cyber Pacifism

Pacifistic movement is usually limited to protest when in conventional weapons domain. But this could change in the cyber space.

Apart from voicing concerns about cyber weapons as discussed in (Rowe, 2007), a more active strategy could be to actively search for vulnerabilities and publicly disclose them as soon as possible. As in the case of cyber disarmament, it would universally destroy the corresponding cyber weapons, hitting the weapons arsenals of many parties simultaneously.

Assuming enough resources are present, the cyber pacifist can have a significant impact on the cyber weapons arsenals of other nation-states without committing any aggressive actions. This again shows how different the cyber weapons world is, leading to new possibilities, but also new limitations.

4.5 Cyber Arms Control

A problem of what to do with cyber weapons found during an inspection as illegal under an Cyber Arms Control treaty is stated by Dorothy Denning (Denning, 2001) . Within our proposed model, the same public disclosure procedure as for *cyber disarmament* could be applied, after the found cyber weapon got analyzed to identify the vulnerability exploited by it . Wherever other copies of discovered cyber weapon are stored, they all rely on the same vulnerability (or same set of vulnerabilities), by disclosing those vulnerabilities one can effectively neutralize each and every of those copies at the same time.

5. Conclusion

Cyber weapons are a new type of armament that follows different rules than the established rules of conventional weapons or weapons of mass destruction. The revolutionary nature of cyber weapons as a means and method of warfare demands the creation of a new conflict model.

This article proposes a highly-simplified, vulnerabilities-based model that defines and describes cyber weapons and cyber defense. The authors analyzed the relationships between hypothetical parties who would develop and employ cyber weapons. The model revealed a number of important findings, such as the fact that a defensive alliance, in which the parties exchanged their knowledge of cyber vulnerabilities, would lead to an enhanced offensive capability by every member of the alliance. Further, the authors proposed a strategy for cyber attack deterrence based on the introduced model. The restricted definition of cyber weapons together with vulnerability-based model has been shown useful for solving cyber arms

control problem, and we hope that the model will show useful in other problems as well.

The examples used in this article primarily highlight the typical roles expected of nation-states, but the authors believe that the model's principles will apply in the corporate world as well.

Acknowledgements

Both authors contributed equally. The opinions shared in this article are those of the authors and do not represent the views of NATO or its member states. The authors would like to thank Mr. Kenneth Geers and Prof. Peeter Lorents who gave us valuable feedback while writing this article.

REFERENCES

Cahill, T., & Rozinov, K. (2003). Cyber warfare peacekeeping. *Assurance Workshop, 2003.*, (June).

Denning, D. (2001). Obstacles and Options for Cyber Arms Control. *Arms Control in Cyberspace, Heinrich Böll Foundation, Berlin, Germany*, 1-13.

Evron, G. (2008). Battling botnets and online mobs: Estonia's defense efforts during the internet war. *Georgetown Journal of International Affairs*, *9*(1), 121–126.

Falliere, N., Murchu, L. O., & Chien, E. (2010). W32. Stuxnet Dossier. *Symantec Security Response*, *3*(November), 1-64. Symantec.

Farivar, C. (2009). A Brief Examination of Media Coverage of Cyberattacks (2007 - Present). In C. Czosseck & K. Geers (Eds.), *The Virtual Battlefield: Perspectives on Cyber Warfare* (p. 183). Amsterdam: IOS Press.

Gjelten, T. (2010). Debating Cyber Disarmament. *World Affairs*. Retrieved from

Herold, R. (2007). DHS Exploding Generator Shows Dire Need For Better Computer Security - Realtime IT Compliance. *www.realtime-itcompliance.com*. Retrieved August 17, 2010, from http://www.realtime-itcompliance.com/information_security/2007/09/dhs_exploding_generator_shows.htm

Hunker, J., & Hutchinson, B. (2008). Role and Challenges for Sufficient Cyber-Attack Attribution. *Science And Technology*, (2003).

Kelsey, J. T. G. (2008). Hacking into International Humanitarian Law : The Principles of Distinction and Neutrality in the Age of Cyber Warfare. *Michigan Law Review*, (May), 1427-1452.

Langner, R. (2011). Keynote speach on Stuxnet @ ICCC 2011. Tallinn: CCD COE Publications. Retrieved January 1, 2012, from http://www.ccdcoe.org/280.html

Lemay, A., Fernandeza, J. M., & Knight, S. (2010). Pinprick attacks, a lesser included case? In C. Czosseck & K. Podins (Eds.), *Conference on Cyber Conflict Proceedings* (pp. 183 - 194). Tallinn: CCD COE Publications.

Mell, P., Scarfone, K., & Romanosky, S. (2007). A complete guide to the common vulnerability scoring system version 2.0. *Published by FIRST-Forum of Incident Response and Security Teams* (pp. 1–23).

Microsoft Collaborates With Industry to Disrupt Conficker Worm. (2009). Retrieved January 3, 2012, from http://www.microsoft.com/presspass/press/2009/feb09/02-12confickerpr.mspx

Miller, C. (2010). Presentation Kim Jong-il and me: How to build a cyber army to attack the U.S. Tallinn: CCD COE Publications.

Moore, T., Friedman, A., & Procaccia, A. D. (2010). Would a'cyber warrior'protect us: exploring trade-offs between attack and defense of information systems. *Proceedings of the 2010 workshop on New security paradigms* (pp. 85–94). ACM.

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

Oiaga, M. (2010). Windows Blue Screens of Death After Patch for 17-Year Old Vulnerability Is Applied. Retrieved August 17, 2010, from http://news.softpedia.com/news/Windows-Blue-Screens-of-Death-after-Patch-for-17-Year-Old-Vulnerability-Is-Applied-134808.shtml

Ottis, R. (2008). Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. *Proceedings of the 7th European Conference on Information Warfare* (p. 163). Academic Conferences Limited.

Ottis, R., & Lorents, P. (2010). Cyberspace: Definition and Implications. *Proceedings of the 5th International Conference on Information Warfare and Security* (pp. 267-270). Academic Publishing Limited.

Rowe, N. C. (2007). War Crimes from Cyber-weapons. *Journal of Information Warfare*, *6*(3), 15–25.

Security, D. O. H. (2010). National Vulnerability Database (NVD) Search Vulnerabilities. Retrieved August 17, 2010, from http://web.nvd.nist.gov/view/vuln/search?execution=e2s1

Sharma, A. (2009). Cyber Wars: A Paradigm Shift from Means to Ends. In C. Czosseck & K. Geers (Eds.), *The Virtual Battlefield: Perspectives on Cyber Warfare* (Vol. 34, pp. 3-17). Amsterdam: IOS Press.

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

Ziolkowski, K. (2010). Computer Network Operations and the Law of Armed Conflict. *Military Law and the Law of War Review*, (49), 47-94.

PUBLICATION II: AN USAGE-CENTRIC BOTNET TAXONOMY

Christian Czosseck and Karlis Podins

Proceedings of the 10th European Conference on Information Warfare and Security,
Tallinn, Estonia 7-8 July 2011, pp. 65-72.

ISBN: 978-1908272065

Abstract: Botnets have been a recognized threat to computer security for several years. On the timeline of malware development, they can be seen as the latest evolutionary step. Criminals have taken advantage of this new technology and cyber crime has grown to become a serious and sophisticated problem which law enforcement still finds difficult to deal with. In the past few years we are witnessing a movement away from cyber crime. Nation states become the target of attacks as well as actively using botnets to project their own power in the political or military domain.

To study the new and emerging cases of botnet usage we propose an usage-centric botnet taxonomy. Although there are already a number of botnet taxonomies published, most of them have a technical viewpoint and often consider cyber crime as the major driver to use botnets. While it may be true for now, we believe that such approach might not be holistic enough to describe the current and future developments. Besides the trend of specialized botnets being developed, the number of botnet users is increasing, with new motivations coming along.

The taxonomy proposed in this paper takes a different viewpoint by focusing less on technical attributes than on the actors using botnets and the functionality requested by them. Major difference from existing research is that proposed taxonomy classifies instances of botnet use. Based on existing taxonomies, case studies of recent botnet incidents and cyber warfare doctrines of selected nation-states, we explore theoretical and already seen ways of botnet usage. We propose new classification of botnets based on their technological attributes, the users and the intended effects on the target to provide a holistic picture of the current situation. We also test the proposed taxonomy on seven instances of botnet use.

Keywords: botnets, taxonomy, incident categorization

Disclaimer
The opinions expressed here are those of the authors and should not be considered as the official policy of the Cooperative Cyber Defence Centre of Excellence or NATO.

1. Introduction

Botnets, large numbers of remote controlled computers distributed all over the Internet and centrally controlled by so-called botmasters, are a persistent and continuously evolving threat to the Internet community, always seeming to be one step ahead of countermeasures and take-down attempts. Over the last years we have seen more and more sophisticated botnets, improving in multiple aspects like size, resistance to countermeasures and ways of spreading. A whole underground economy developed around botnets (Klein et al. 2011). More and more botnets have become a service offered by knowledgeable malware developers, ready to be rented out to everyone willing to pay (Schwartz 2010; Mills 2009). Besides technological evolution, the number of players as well as their motivations to use botnets is increasing. The recent history has witnessed several incidents where botnets were not used for financial benefit, but to deliver a political message, to conduct espionage or as an instrument for sabotage. The increasing diversity of botnet incidents requires for a structured botnet classification.

The usage-centric botnet taxonomy presented in this paper is designed to classify botnet events by means of usage, not botnets per se. By this our approach differs from other published taxonomies on botnets, which mostly focus on technical aspects.

The rest of this paper is structured as following: In section 2 we give an overview on related work of botnet taxonomies, motivating the uniqueness of our taxonomy; it will be described in the following section 3. We test the performance of the proposed taxonomy in Section 4 by categorizing a selection of recent botnet incidents according to it. Finally the conclusions and a discussion of future work are provided in Section 5.

2. Related work

Technical details of botnets and their highly visible functionality like DDoS attacks are well studied in scientific literature. But strategic aspects like motivation are rarely covered. (Weaver et al. 2003) present the *Taxonomy of Computer Worms.* They introduced *payload* and *motivation* attributes similar to the *functionality* and *motivation* attribute presented in this paper's taxonomy. (Weaver et al. 2003) present a more fine-grained classification in their features. On the other hand we separate users from their motivation, being combined to one in (Weaver et al. 2003). They also do not consider self-infection.

Detailed technical-level taxonomy of attacks and thorough literature review of technical-level taxonomies is given by (Hansman & Hunt 2005).

A technical defense-centric taxonomy of computer attacks is given in (Killourhy et al. 2004), where the authors discuss network level attack detection and classification. Several attack types like Denial of Service and Surveillance/Probing (corresponds to Information theft in the proposed taxonomy) are discussed in (Lippmann et al. 1998). (Distributed) Denial-of-Service (DDoS/DoS) attacks have been studied by (Lau et. al, Distributed Denial of Service Attacks). (Wun et al. 2007; Asosheh & Ramezani 2008; Wood & Stankovic 2004) offer taxonomies not limited to DDoS as such but covering architectural aspects of botnets like command-and-control structures or spreading strategies. Taxonomies of DoS attacks and countermeasures against them have been presented by (Champagne & Lee 2006; Mirkovic & Reiher 2004). A more detailed description of botnets internals including a comprehensive list of way how to use botnets several kinds of botnet usage) is presented by (Bacher et al. 2005; Barford & Yegneswaran 2007)The fast flux functionality provided by some botnets is covered in (Holz et al. 2008) and (Jose Nazario & Holz 2008).

Majority of research has considered botnets as collections of machines which are infected without the knowledge or consent of the respective owners (Klein et al. 2011). Recently in a small number of politically-tainted incidents botnet software has been installed intentionally by the owners (Ottis 2008; Panda Security 2010).

3. An usage-centric botnet taxonomy

Following the criteria for an effective taxonomy as introduced in (Killourhy et al. 2004), our taxonomy was designed to follow the principles of be *mutual exclusiveness*, *exhaustiveness* and *replicability* providing an instrument to classify botnet incidents of the past but also to deal with upcoming events.

It consists of four features: 1. Users of botnets, 2. Motivations of botnet usage, 3. Functionality applied, and 4. Way of infection. A complete overview is provided in figure 1.

3.1 Users of botnets

Over the past years, developing and using botnets have become a profitable business. A well developed underground economy, providing botnet technology and services to everyone who pays (Mills 2009). The easy access to botnets introduces new players and motivations to appear. The first attribute of this taxonomy covers the user of the botnet and is motivated by a legal viewpoint considering who could be held liable for the action done.

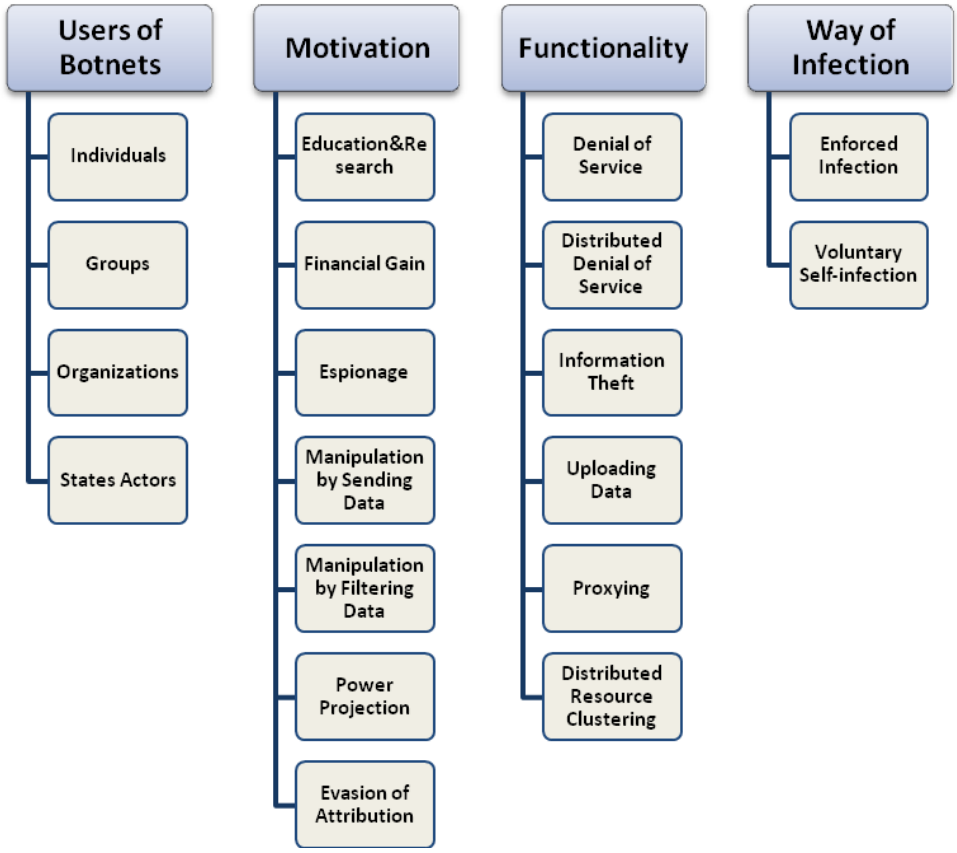

Figure 9: Usage-centric Botnet Taxonomy

Exclusion of middlemen

Over the time it has been witnessed that the underground economy has changed to a new service-oriented model, offering botnets for rent (Schwartz 2010; Mills 2009). This way a third party besides botnet user and the target gets involved. While these servicemen are important players, our taxonomy focuses on the perpetrator only. *We disregard the involvement of middlemen in the incidents, although they might be held responsible for the damages caused.*

Individuals are private persons using botnets independently. This includes private persons using botnets for financial gain, education or out of curiosity. But also those, who want to express their opinion with digital force or support a political or ideological activity e.g. patriotic hacking, as in the case of the cyber attacks against Estonia in 2007 (Ottis 2008) or participants in the Operation Payback (Correll 2010). From a legal viewpoint, it is the individual who could be made responsible.

Groups shall cover all forms of collaborative and coordinated, but still loose group of individuals. It does not include groups formed based on a legal person (e.g. a company), and as such leaves only every single individual as being responsible for their actions. Persons with different roles might face different consequences, though. This covers examples where a group of persons were acting as a whole and out of internal motivation, as seen to a certain part in the Operation Payback incident with regards to the role of *Anonymous* (Panda Security 2010) and the later founded *AnonOps* (AnonOps 2010).

Groups also include examples of organized crime organizations, which do not use a legal body as a facade.

Organizations, in contrast to groups, are mainly defined by the legal person representing them. Beside of the individuals within the organization (and their personal liability), there is a legal person according to private law, which can be made responsible. This covers all companies using botnets for e.g. getting an (economic) advantage over another party, and to a limited extent on organized crime, if they also use a legal person for conduction at least parts of their operations. This class shall also include organizations established under international, private law.

State Actors are the type of users this taxonomy defines, and shall cover all organizations established under public national or international law. These include esp. parts of the executive power of a state, like police, military or intelligence services.

3.2 Motivations for botnet usage

Botnets are powerful and flexible tools providing their user with wide variety of functionality. While many different features of the botnet can be used at the same time, they are connected by the single motivation of the perpetrator at the time of usage. The second attribute provides the following broad classes of motivation behind botnet usage, which are similar to Motivations and Attackers identified by (Weaver et al. 2003).

Education & Research covers all activities done for the sake of getting familiar with the botnets, independently if one is interested in using, developing, analyzing or defending against botnets. The key attribute for this taxon is absence of a clear target e.g. violate somebody's rights or property.

Seeking *Financial Gain* is maybe the most common motivation for using botnets nowadays. This includes most cases of *information theft*, like stealing bank or credit cards information or license keys, as this information will be monetized nearly immediately by either using or selling it.

Espionage covers all cases where stolen information is not intended to be turned into money directly or at all. Instead, the gathered knowledge is used to influence own decisions, the relationship between parties or to enhance an own situation awareness. This taxon is independent from the *User of the Botnet* as defined in the previous section and as such covers e.g. cases of state spying or industrial espionage.

The *Manipulation by Sending Data* is an umbrella class for all cases of botnet usage, where an outward directed data flow (from the viewpoint of the infected machine) is used a) to expression one owns opinion on something; or b) to manipulate someone other's opinion by sending wrong or misleading information.

The first sub-category covers cases like *hacktivism* (Denning 2001; Ottis 2008), where groups of persons use botnets to attack others, e.g. disturbing normal functionality of provided services, to support their political message. The second sub-attribute covers cases of propaganda or manipulation of services or outcomes of polls or voting, leading to a wrong final picture for others (Temmingh & Geers 2009a).

On the other hand *Manipulation by Filtering Data* shall cover all cases where denying access to information is the main reason for the botnet usage. This covers cases of censorship (see e.g. the Belarus case in Pavlyuchenko 2009), information blockages or redirection.

Botnets can be used as an instrument to *Project Power* in cyber space. To adopt Clausewitz freely, botnets can be used as a tool to influence another party's behavior or policy, after non-violent options are exhausted. This shall include, but not be limited to cases where botnets became part of *military operations* (e.g. the InfoOp against Georgia friendly news portals and governmental websites descried in J. Nazario, 2009), or could be used to damage another's economy (Lemay et al. 2010). We also include cases of *sabotage* (like in the case of Stuxnet, see Falliere et al. 2010), or blackmailing (Sophos 2006) to be included here. It needs to be stressed here, that this taxon is independent from the user of botnets and as such reaches from individuals to state actors.

To *Evade Attribution* is one other reason one might want to consider using botnets. The mostly global distribution of botnets allows the user to let its victim believe that someone else was behind the cyber attack. This can even be extended to the intention to run a *false flag operation*. While botnets are not the only possible way to reach this goal, it is for sure a convenient one. As transnational cooperation in fighting cyber crime is still not developed globally, and not all nation states enjoy friendly relationships, disguising one real location and identity can be the reason to use botnets. Another scenario included is the (massive, distributed) *acquisition of resources.* Here the availability of the sheer number of zombies in the botnets, and with it the combined CPU processing power or storage capacity is used to set up a distributed service, there any single node does not have enough knowledge

so that even if forensically analyzed, the service as a whole is not endangered or compromised.

3.3 Functionality

The functionality provided by a botnet is highly dependent on the developer of the botnet and can vary quite significantly between botnets. A fundamental feature of all botnets is the ability to remotely control computers and the ability to send files to them, e.g. for updating the bot client later on. On top of this a variety of different functions has been developed and became part of many botnets, while not all share always the same features. As of the common update feature, enhancing a botnet's capabilities later on is most often possible.

The third attribute of this taxonomy provides a set of generic features botnets might have. It combines features already seen in botnets over the past years, and also some new ones, the authors believe them to be reasonable to consider as they might been seen in the near future.. While this list has been prepared with care, based among others on (Weaver et al. 2003; Bacher et al. 2005), this is not claimed to be complete. The future might show new functionality not thought of till now.

Denial of Service (DoS) is the ability to disrupt the normal functionality *of the infected machine* as a whole. This enables the botnet master to shut down or even damage the infected system, making a recovery at least difficult.

Distributed Denial of Service (DDoS) is a functionality whereby a large number of service requests are directed to a target system, exhausting its available resources to especially answer to desired requests. For these attacks, the number of used botnet clients is the main criteria for the success of the DDoS, while is recognized that more sophisticated attack techniques might lead to a lower number of necessary bots to attack the target.

Information theft of data stored or processed on the infected machine or traffic passing or reaching it is another commonly seen functionality of botnets (Klein et al. 2011). This includes but not limits to the search for specific files, passwords or other sensitive data stored or typed into the infected workstation, e.g. banking credentials.

Uploading data, as the opposite of information theft, enables the botnet owner to deliver any desired file onto the infected machine. A basic implementation of this functionality is most often standard for all botnets, as it is necessary to *update* the installed malware. Beside this, the installation of additional software, e.g. further spyware, advertisement add-ons, or Browser Helper Objects is frequently seen (Bacher et al. 2005). In a bigger scale this could be used to implement a regional surveillance system (see e.g. the idea presented in Husted & Myers 2010).

But the botnet owner is not limited to, as he can basically upload any file he wants to the infected machine, and as such could e.g. place compromising or illegal data. Another special case of this taxon is the use of the botnet as a launch platform for other malware, accelerating its spreading by magnitude or enables regional targeted distribution of it like in the case of Stuxnet (Falliere et al. 2010).

This also includes the manipulation of existing files on the infected system to change their intended functionality. It is e.g. not uncommon for malware to disable running AV software or restricting access to AV websites (Porras et al. 2009).

Proxying is the ability to use the infected clients to execute actions on behalf of the botnet master, without him being revealed directly. Known cases are *Spam campaigns*, where the bots as tasked to send massively emails to a target group. Using a limited number of bots to form a *proxy chain* can provide functionality similar to anonymization services like the TOR network, where tracking traffic routes is close to impossible. Or they are used to hide the real location of some critical services, like phishing site or C&C servers, by implementing *fast-flux domains* (Jose Nazario & Holz 2008). Another not often seen way of using this functionality would be the *manipulation of voting* (Temmingh & Geers 2009b) or *click-based (advertisement) services* (Bacher et al. 2005).

Distributed resource clustering is a newly introduced function not commonly used so far. But the authors believe that there is room for botnet herders to explore this area more. It is understood that all the other mentioned functions also use resources of the infected machine to execute the mission they are tasked with. This taxon of botnet usage assume the botnet herder to combine the available resources, namely CPU time or HDD space to build a service like known from the domain of clustered computing or cloud computing. The resource made available this way would enable him e.g. to conduct distributed calculations which could be useful for password cracking or to set up a distributed storage, where any member of the botnet holds part of the data the botnet herder wants to store. If designed well he could store huge amount of data, redundant and segmented in the botnet without any single bot client having enough parts for reconstruction a complete picture.

3.4 Way of infection

Enforced Infection:
Most botnets usually behave like any other malware trying to infect as many hosts as possible, spreading autonomously if ordered to do so. Computers are infected and join botnets without the knowledge or consent of the owner. Malware developers are actively developing and looking for new exploits to infect new hosts, and so far they are quite successful (Klein et al. 2011)

Voluntary Self-infection:
Besides the mentioned common way of infection, there have been a number of cases when owners voluntarily infected their machines to join a botnet. By doing

that they supported a certain (politically motivated) cause, e.g. incidents in Estonia 2007 and Operation Payback 2010 (Ottis 2008; Panda Security 2010).

4. Application of the taxonomy

In order to test how well the taxonomy classifies events of botnet usage, we look at a selection of recent incidents involving botnets. These events are chosen to represent a wide variety of botnet uses; their order does not reflect any sort order of importance. In some cases, several closely-related incidents are classified together as a group, because different events using the same bots happened at the same time. An overview is presented in Table 1.

4.1 Stuxnet

Although the number of Stuxnet infected hosts was small and spreading was highly targeted, the most basic features of botnets being the existence of a command and control capability support to consider Stuxnet as a botnet (Falliere et al. 2010).

While categorizing this incident using the proposed taxonomy, the lack of trustworthy, full information left the attribute of Users of Botnets hard to decide. While there are many speculations on this, we decided to assume at least one *state actor* being involved. The Motivation is covered by the *power projection* taxon including sabotage, which seems to be the most likely motivation behind this incident. Stuxnet spread by involuntary infection, and its manipulation and damaging industrial systems represents a *denial of service* functionality.

4.2 GhostNet

There is no evidence on who are the players behind GhostNet. Speculations reach from (groups of) individuals up to state actors. As such we leave the user as *unknown*. But the small number of infected hosts (around 1300) and percentage of high-value targets (up to 30% of infected hosts belonged to ministries of foreign affairs, embassies, international organizations etc.) indicate that the motivation was espionage against pro-Tibet community. In order to do that, GhostNet was performing information theft from involuntary infected machines (Deibert et al. 2009).

4.3 Operation Payback

The *Operation Payback* was launched by a *group* of WikiLeaks supporters, after multiple financial service providers stopped their services for WikiLeaks after the latest, massive disclosure of classified US documents.

The attacks were carried out by using an open source network attack application called Low Orbit Ion Cannon. The attacks were coordinated by using internet forums, Twitter and some C&C servers (Pras et al. 2010; Panda Security 2010; Correll 2010). According to our taxonomy, we classify the motivation as *projecting power*. The functionality of choice was *DDoS* attacks and the participation in this event was *voluntarily*.

4.4 Help-Israel-Win

A *group* of pro-Israel activists, in their campaign against Hamas (*power projection*) set up a website also hosting software for download, to *voluntarily* join a botnet under the control of this group. Based on the information released by this group, they use the botnet to conduct *DDoS* attacks against pro-Palestinian web sites. To which extend they were successful, or if they have launched any attacks at all is still unclear (Shachtman 2009).

4.5 Conficker

Till now it is publicly not known, who the developers and users of Conficker are. But the analysis of this malware and the speed with which this botnet adapted to counter measures lets us assume, that at least a *group* of persons is behind Conficker. The *lack of any executed functionality* beside file transfer to update the infected clients with last versions of Conficker allows the assumption that Conficker was mainly developed as a proof-of-concept and as such falls under *Education&Research*. Conficker infected its host *involuntary* (Porras et al. 2009).

4.6 Mariposa

The Mariposa botnet, claimed to be one of the world's largest botnets ever, was developed and used by an international *group* of criminals for *financial gain*. They harvested banking credentials and credit card data (*information theft*) as well as used it for launching *DDoS* attacks. The victims were all infected *involuntarily* (McMillan 2010).

4.7 Belarus censorship

The Belarus state has a longer history of enforcing Internet censorship on its citizens with regards to regime-critical information. Chapter '97, a leading venue for public discussions in Belarus, suffered regularly under state sponsored cyber attacks against their website. In April, 2008 *DDoS* attack took them down to block state-independent news coverage of protest ongoing in the streets (*manipulation by filtering data*).

While Belarus officials denied official involvement, it is assumed that they were not actively countering the attacks. As such we classify this incident as done by a

state actor. As the used botnets are unknown, the infection way cannot be decided upon (Pavlyuchenko 2009).

Table 1: Overview of selected incidents and their classification.

Example	**User**	**Motivation**	**Functionality**	**Way of infection**
Stuxnet	State Actor	Power Projection	Denial of Service	Involuntary
GhostNet	Unknown	Espionage	Information theft	Involuntary
Operation Payback	Group	Power projection	DDoS	Voluntary
Israeli	Group	Power Projection	DDoS	Voluntary
Conficker	Group	Education&Research	none	Involuntary
Mariposa	Group	Financial Gain	Information Theft/ DDoS	Involuntary
Belarus Censorship	State Actor	Power Projection	DDoS	Unknown

5. Conclusions

Easy access to botnets makes them available to all kind of parties, not all of them particularly interested in monetary revenue, but increasingly pursuing political and military aims. With this the common interpretation of monetary motivated cyber crime being the main driver behind the usage of botnet does not sufficiently cover the current situation anymore.

We have presented a usage-centric taxonomy, which provides a structured approach to compare different botnet incidents.

Two distinct applications of the proposed taxonomy were considered; firstly to analyze and categorize past and current botnet incidents. The applicability of the taxonomy has been shown on a selection of recent botnet incidents. The performance of the usage-centric taxonomy in classifying the selected incidents gives hopes that the proposed taxonomy will be helpful in understanding other botnet incidents. This might motivate to structure countermeasures in a similar way and developing an instrument to organize and select responses on different levels.

Another application is to help thinking about novel ways of using botnets. By pre-selecting some attributes, the taxonomy allows for structured and systematic search thru the remaining attributes. By this, the taxonomy might find interesting and novel botnet-related threats and lead to improvements of existing or forthcoming risk assessments and as such helps to improve cyber security on institutional down up to national level.

This taxonomy was designed defining generic taxon, able to be matched even future incidents and is believed to cover most seen so far. Nevertheless the future might show the need to amend the list of taxa, especially the one of *Functionalities applied*.

Bibliography

AnonOps, 2010. Welcome to AnonOps Network | Anonymous Operations (AnonOps), HACKERS ON STEROIDS. Available at: http://www.anonops.ru/ [Accessed February 9, 2011].

Asosheh, A. & Ramezani, N., 2008. A comprehensive taxonomy of DDoS attacks and defense mechanism applying in a smart classification. *WSEAS Transactions on Communications*, 7(4), pp.281-290.

Bacher, P. et al., 2005. Know your enemy: Tracking botnets. *The Honeynet Project*.

Barford, P. & Yegneswaran, V., 2007. An inside look at botnets. *Malware Detection*.

Champagne, D. & Lee, R., 2006. Scope of DDoS countermeasures: taxonomy of proposed solutions and design goals for real-world deployment. *on Systems and Information Security (SSI)*.

Correll, S.-P., 2010. 'Tis the Season of DDoS – WikiLeaks Edition | PandaLabs Blog. *Pandalabs*. Available at: http://pandalabs.pandasecurity.com/tis-the-season-of-ddos-wikileaks-editio/ [Accessed February 9, 2011].

Deibert, R. et al., 2009. Tracking GhostNet: Investigating a Cyber Espionage Network. *Information Warfare Monitor, Munk Centre, JR02-2009, March*, 29.

Denning, D.E., 2001. Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy. *Networks and netwars: The future of terror, crime, and militancy*, p.239–288.

Falliere, N., Murchu, L.O. & Chien, E., 2010. W32. Stuxnet Dossier. *Symantec Security Response*, 3(November), pp.1-64.

Hansman, S. & Hunt, R., 2005. A taxonomy of network and computer attacks. *Computers & Security*, 24(1), pp.31-43.

Holz, T. et al., 2008. Measuring and detecting fast-flux service networks. In *Symposium on Network and Distributed System Security*. Citeseer.

Husted, N. & Myers, S., 2010. Mobile location tracking in metro areas: malnets and others. In *Proceedings of the 17th ACM conference on Computer and communications security*. ACM, p. 85–96.

Killourhy, K.S., Maxion, R. a & Tan, K.M.C., 2004. *A defense-centric taxonomy based on attack manifestations*, IEEE.

Klein, G., Leder, F. & Czosseck, C., 2011. On the Arms Race Around Botnets - Setting Up and Taking Down Botnets. In C. Czosseck & K. Podins, eds. *2011 3rd International Conference on Cyber Conflicts*. Tallinn: CCD COE Publications (in press).

Lemay, A., Fernandeza, J.M. & Knight, S., 2010. Pinprick attacks, a lesser included case? In C. Czosseck & K. Podins, eds. *Conference on Cyber Conflict Proceedings*. Tallinn: CCD COE Publications, pp. 183 - 194.

Lippmann, R.P. et al., 1998. Evaluating intrusion detection systems: the 1998 DARPA off-line intrusion detection evaluation. *Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00*, pp.12-26.

McMillan, R., 2010. Spanish police take down massive mariposa botnet. *IDG News*. Available at: http://www.pcworld.com/businesscenter/article/190634/spanish_police_take_down_massive_mariposa_botnet.html [Accessed February 9, 2011].

Mills, E., 2009. Golden Cash?network - rent a botnet - ZDNet. *CNET News*. Available at: http://www.zdnet.com/news/golden-cash-network-rent-a-botnet/312957 [Accessed February 9, 2011].

Mirkovic, J. & Reiher, P., 2004. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2), p.39.

Nazario, J., 2009. Politically Motivated Denial of Service Attacks. In C. Czosseck & K. Geers, eds. *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam: IOS Press, p. 2010–05.

Nazario, Jose & Holz, T., 2008. As the net churns: Fast-flux botnet observations. In *Malicious and Unwanted Software, 2008. MALWARE 2008. 3rd International Conference on*. IEEE, p. 24–31.

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*. Academic Conferences Limited, p. 163.

Panda Security, 2010. The Anonymous cyber-activist group, responsible for the attack on Spain's SGAE and other copyright societies, launches further attacks in defense of Wikileaks founder | Press Panda Security. *Panda Security*. Available at: http://press.pandasecurity.com/news/the-anonymous-

cyber-activist-group-responsible-for-the-attack-on-spain's-sgae-and-other-copyright-societies-launches-further-attacks-in-defense-of-wikileaks-founder/ [Accessed February 9, 2011].

Pavlyuchenko, F., 2009. Belarus in the Context of European Cyber Security. In C. Czosseck & K. Geers, eds. *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam: IOS Press.

Porras, P., Saidi, H. & Vinod, Y., 2009. *An Analysis of Conficker*,

Pras, A. et al., 2010. *Attacks by ?Anonymous ?WikiLeaks Proponents not Anonymous*,

Schwartz, M.J., 2010. Pssst...Want To Rent A Botnet? - Darkreading. *Dark Reading*. Available at: http://www.darkreading.com/security/vulnerabilities/225200525/index.html [Accessed February 9, 2011].

Shachtman, N., 2009. Wage cyberwar against hamas, surrender your pc. *Wired*. Available at: http://www.wired.com/dangerroom/2009/01/israel-dns-hack/ [Accessed February 11, 2011].

Sophos, 2006. Online Russian blackmail gang jailed for extorting $4m from gambling websites. *Sophos.com*. Available at: http://www.sophos.com/pressoffice/news/articles/2006/10/extort-ddos-blackmail.html [Accessed February 9, 2011].

Temmingh, R. & Geers, K., 2009a. Virtual Plots, Real Revolution. In C Czosseck & K Geers, eds. *The Virtual Battlefield: Perspectives on Cyber Warfare*. IOS Press, pp. 294-302.

Temmingh, R. & Geers, Kenneth, 2009b. Virtual Plots, Real Revolution. In Christian Czosseck & Kenneth Geers, eds. *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam: IOS Press, pp. 294-302.

Weaver, N. et al., 2003. A taxonomy of computer worms. In *Proceedings of the 2003 ACM workshop on Rapid Malcode*. ACM, p. 11–18.

Wood, A. & Stankovic, J., 2004. A taxonomy for denial-of-service attacks in wireless sensor networks. *of Sensor Networks: Compact Wireless and*.

Wun, A., Cheung, A. & Jacobsen, H.-A., 2007. *A taxonomy for denial of service attacks in content-based publish/subscribe systems*, New York, New York, USA: ACM Press.

PUBLICATION III: ON THE ARMS RACE AROUND BOTNETS – SETTING UP AND TAKING DOWN BOTNETS

Christian Czosseck, Gabriel Klein and Felix Leder

Proceedings of the 3rd International Conference on Cyber Conflict, Tallinn, Estonia
7-10 June 2011, pp.107-120

ISBN: 978-9949-9040-2-0

Abstract: Botnets are a well-recognized and persistent threat to all users of the Internet. Since the first specimens were seen two decades ago, botnets have developed form a subject of curiosity to highly sophisticated instruments for illegally earning money. In parallel, an underground economy has developed which creates hundreds of millions of euros per year in revenue with spamming, information theft, blackmailing or scare-ware. Botnets have become a high-value investment for their operators that need to be protected from law enforcement agencies or the anti-botnet community. Security researchers and companies trying to keep them within bounds are facing the very latest in spreading and defense techniques. Hundreds of thousands of new malware samples per month pose an immense challenge for AV companies. Specialized countermeasures against botnets have evolved along with botnet technology, trying to bring them down by targeting the root of every botnet: its command-and-control structure. This leads to an ongoing arms race between botnet developers and their operators vs. security experts. So far the former have the upper hand.

Based on the analysis of multiple botnet takedowns and the in-depth investigation of various botnet architectures conducted by the authors, this paper provides an analysis of the efforts needed to acquire and set up a botnet. This is followed by a comparison of selected significant botnet countermeasures, which are discussed with regard to their required resources. Legal and ethical issues are also addressed, while a more thorough discussion of these will be left for future work.

Keywords: IT security; botnet; malware; infection; disinfection; botnet setup; botnet takedown; tactical takedown

1. Introduction: Current State of the Arms Race

Botnets are networks of computers infected with malicious software (malware), remotely controlled by so-called bot herders. The infected machines within this botnet (a.k.a. bot or zombie) are regularly abused to perform mostly criminal activities without the knowledge of their owners. This includes but is not limited to sending spam, conducting distributed denial-of-service (DDoS) attacks or harvesting sensitive data such as credit card credentials. Beyond credit card fraud, extortion schemes can also be observed with threats of large-scale DDoS attacks unless payments are made. All this leads to steadily increasing financial damage and cyber crime's yearly income surpassing the global drugs revenue [1]. As a latest trend, botnets play an increasing role in politically motivated attacks against

public and private institutions, sometimes threatening entire countries [2]. Behind this is a well-developed underground market, on which botnet technology and associated services are sold to everyone at rather low prices [15].

Anti-virus (AV) companies as the natural enemy of malware are constantly trying to keep up with the growing threat, developing a variety of products to protect computers from being infected. Unfortunately, malware authors are often one step ahead because of the reactive defense provided by AV software. If newly developed malware is released, even up-to-date anti-virus detectors are often not likely to detect it [3]. Some AV software detects less than 10 % of new samples within the first 24 hours of their occurrence. Often manual analysis of new malware samples is required because automatic approaches are limited in their capabilities. There is a general consensus in the AV industry that current solutions are neither scalable nor sustainable enough.

Acknowledging the fact that malware spreading cannot be stopped or slowed down significantly, other countermeasures directly attacking established botnets have been developed.

To receive or pass on commands, the individual parts of these botnets need to communicate with each other and with their so-called command-and-control (C&C) servers. The method according to which this communication takes place defines the topology of the botnet. So far three different ones have been established: centralized topologies with few C&C servers, decentralized topologies based on peer-to-peer (P2P) protocols, and semi-flexible topologies often realized by fluxy domain registrations.

If connectivity between bots and C&C servers is established, different communication protocols like HTTP or IRC are commonly used. A more in-depth discussion of technical botnet issues can be found in [4] and [5]. All these technical aspects provide entry vectors for targeted counter measures against botnets.
This paper provides a comprehensive overview of the resources needed in this arms race between bot herders and botnet hunters. Based on analyses of recent botnet investigations and experience from conducted takedowns, the most common countermeasures are presented and analyzed.

The paper discusses the countermeasures with regard to their required resources, namely *required skills*, *monetary costs* and *time* as well as the *likelihood of a successful* takedown. Legal and ethical aspects are also addressed. The discussion is based on a simple taxonomy of botnets presented in Section 2, grouping botnets into three broad groups. In Section 3, we discuss the efforts needed to set up a botnet for each of the introduced categories. This is followed by an in-depth discussion on required resources for the most common botnet countermeasures in Section 4. We conclude with a summary and an outlook on future developments.

2. Botnet Evolution

Since the world fist encountered a computer virus called Brain back in 1984, malware has developed from a proof of creativity to a highly sophisticated instrument usable for various tasks, nowadays aiming mainly for earning money in a criminal way.

Botnets themselves evolved from the idea of a massive remote control for administrative tasks to a flexible type of malware encompassing the most successful spreading and hiding techniques.

Botnets evolved and became more professional over time. This is reflected in their capabilities, but also in the skills needed for their creation. Nowadays, experienced and knowledgeable malware developers are needed to create botnets which are hard to detect or to mitigate.

This paper introduces three broad categories of botnets reflecting the major evolutional steps over the past decades. The discussion on setting up or taking over/down botnets is structured according to these categories.

A. Open-Source Botnets

The first category is formed by botnets that were either developed open-source, were made freely available later on, or are easy to find. This marks the very beginning of malicious botnet development, where botnets and malware in general was often written for (often still illegal) fun or out of competition between "geeks." Monetary aspects were hardly a driving force.

Well-known representatives are botnets like AgoBot, SDBot or RBot [22, 23]. While quite old, they are still in use and are sometimes developed further by single groups adding new exploits or functionality. These new exploits are developed individually or obtained from other sources like the exploit framework Metasploit [6]. For this category we assume that most of the code base is freely available for both malware developers and AV companies. They are easy to set up, typically only requiring the botherder to make some changes in provided configuration files and compiling the code.

An alternative way of operation is the development of a closed-source botnet (which might be a fork of or inspired by an existing open-source botnet), adding well developed open-source components to the code base. Popular examples for open-source components integrated into closed-source botnets are cryptographic and compression routines. Waledac used the OpenSSL library [4, 7], for both RSA and AES, Conficker included the official MIT implementation of the MD6 hash algorithm [8], and Storm made use of the zlib [9] compression library [24]. This provides malware developers with reliable, well tested standard routines, reducing their efforts. If a particular botnet is a fork of one of the older open-source botnets

mentioned above, we consider it to fall under this category. Otherwise the botnets belong to one of the following categories.

B. Construction Kit-based Botnets

Over time, botnets developed into an effective tool to illicitly earn money. With AV and other security companies putting more efforts into fighting botnets, botnet developers improved resistance to countermeasures. However, they invented an increasing number of new features for generating money, e. g. by harvesting financial credentials or other valuable information and subsequently selling them later. Botnet developers started to understand the value of their creations and that not everybody is able to develop sophisticated botnets, thus raising the value of well-developed ones. Out of this a business model developed in an underground scene, where botnet developers started to sell botnet software. To an increasing extent, this is offered together with patch services, infection guarantees and/or hosting services. Botnets became available as so-called constructions kits, enabling everyone to configure and create their own botnet in a point-and-click fashion.

This category covers all botnets fitting this description. They are assumed to be well maintained, regularly updated, and coming with the ability to add new functionality (add-ons), maybe even by third parties. Many of them are sold including support for the buyer via ICQ or other digital media. These botnets are normally developed as closed source, using state-of-the-art methods, software development processes and quality assurance methods [10]. To protect the botnet software, licensing schemes and code protection software such as VMProtect [11], commonly encountered in legitimate software products, are used to control the distribution of their products. This makes analyzing or stealing the botnet's source code hard for competitors and AV companies.

Prominent examples of botnets that are sold as construction kits are ZeuS and its presumable successor, SpyEye, both targeting financial data. In the case of ZeuS, the C&C server is provided based on open-source components written in PHP. Prices usually range from a few hundred to several thousand USD depending on the feature set [15].

C. Specialized Botnets

The last category this paper introduces covers all botnets, which were developed with a very specific target or functionality in mind. While most of the attributes of the second category still apply, specialized botnets are highly professionally developed, combining advanced expertise in exploit development (e. g. by usage of 0-day exploits), careful software engineering considering latest countermeasures, and sometimes even combine cross-domain knowledge or intelligence of the target. Monetary gains as a driving force might but do not need to be present. Espionage and sabotage are other motivations for this advanced persistent threat (APT).

Examples for this category are Ghostnet [12], which aimed at political espionage in China-critical communities, or Stuxnet, which was developed to target Windows-based supervisory control and data acquisition (SCADA) systems and is assumed to be an instrument of information gathering and sabotage of the Iranian nuclear program [13]. Night dragon is a botnet spying mainly on petrol and gas companies [25]. Another example is Conficker, which, while actively developed to be impervious to latest countermeasures and widely spread, still has not shown any active functional payload.

3. Setting up a Botnet

In 2008, spammers alone earned an estimated 780 million USD [14] and there is an upward trend to these numbers. With this ever increasing amount of money to be made by operating or renting out botnets, an increasing professionalization in the domain can be observed [26]. Structures similar to free market (sub-) economies are emerging where prices and the availability of products and services are regulated by demand. There are even marketing campaigns on underground forums promoting certain products. Taking these issues into account, what are the resources that remain to be expended for setting up and deploying a botnet? In this section we will discuss these resources in the context of the botnet categories introduced in the previous section.

A. Finances

As the development of open-source botnets is community-driven, no direct monetary cost is involved. Depending on the situation, software developers might need to be paid.

The prices of construction kit botnets vary; entry-level ZeuS kits can be purchased for 3,000-4,000 USD, whereas more advanced kits can cost more than 10,000 USD [15]. Additionally, appropriate infection kits can be bought from 100 to more than 1,000 USD [16]. A range of companies exist that provide “all-inclusive” packages for botnet construction, propagation with exploit kits, as well as command-and-control server hosting and maintenance.

Where specialized botnets are concerned, especially skilled and trusted developers are required. Components are typically self-developed and seldom purchased. The required trust and skill level makes these types of botnets more expensive than extensions to open-source botnets. In case of sabotage and for reliable development, test environments have to be bought, set up, and maintained [13].

B. Development Skills

There are three aspects to be considered when developing a botnet: the infection of the target machine, the botnet binary that is executed on the target machine after infection, and the C&C infrastructure. Different development skills are required

for each aspect. Resource requirements for infection are fairly similar for the different classes of botnets and are discussed in a subsequent section.

To configure and install the bot component of an open-source botnet, the user needs a basic understanding of source code configuration and needs to be able to use a compiler. A non-technical user can acquire these skills in a short amount of time. However, a risk in this case is the unknown programming quality of the malware.

Compared to this, the configuration and setup of construction kit botnets is almost negligible. These kits are for sale and designed with user-friendliness in mind. The entire process takes only a few clicks of the mouse. Configuration is accomplished easily by adapting existing configuration files or purchasing ready-made ones. Most kits come with a standard set of system manipulations.

With specialized botnets, the greatest difficulty lies in the amalgamation of cross-domain knowledge. This does not usually apply to botnets in the other groups. Specialized botnets have highly customized goals, e. g. espionage or sabotage. Exploiting weaknesses and optimizing malware for execution in systems in these environments requires a high degree of immersion in that context. An example of this is Stuxnet. Here, a detailed familiarity with very specific industrial control systems was required. The actual technical skills are comparable to those required for open-source botnets, although in most cases there is no software base to build upon so extensive development effort is needed. An additional difficulty is that community support cannot be relied on here.

Where the development of C&C infrastructure is concerned, construction kit-based botnets require the least effort of the three classes. In principle, setting up a C&C server is identical to setting up any other content-management system. For a more in-depth discussion of C&C infrastructures, please refer to [4]. Protecting the C&C server against takedown attempts by authorities and security researchers is more challenging, but often all-inclusive bundles are offered that include setup, support and bulletproof hosting of the C&C server. For open-source and specialized botnets, these activities have to be performed manually.

C. Defensive Skills

To protect their software from reverse engineering and analysis, malware authors increasingly employ defensive measures on a technical level.

An often-used mechanism is encryption, both of the communication with the C&C server and of the malware binary itself. Circumvention of the former is always possible. This is an imminent weakness in botnets using encrypted communication because the encryption keys either need to be included in the binary or can be observed when processed in the binary during runtime.

Obfuscation is a technique for hiding that different malware samples belong to the same botnet and to complicate detailed analysis of the internals. A recent trend is

so-called server-side polymorphism. Here, the server from which a newly infected machine retrieves the actual malware encodes the binary differently for every client. This can include differences in the encryption routine, encryption keys, etc. The result is that binaries from two different infected hosts have nothing in common at first glance.

Already existing malware can be precisely immunized against certain AV products or analysis tools. This can easily be done manually because of Web sites such as VirusTotal, a meta-anti-virus tool that allows the online scanning of malware samples with multiple AV solutions. Malware can also be hardened automatically using third-party tools.

By implementing blacklists of IP addresses of known honeypot or other analysis systems, malware developers can explicitly avoid infecting malware analysis systems. Knowledge about such systems can be gathered in a variety of ways. A Web site called AV Tracker [18] contains a comprehensive list of sandboxes, Honeypots and other analysis systems operated by the AV industry and malware researchers world-wide. Going one step further, ZeuS operators have been observed to set up a honeypot-like system to analyze and provide further information about researchers trying to infiltrate its administrative interface [19].

In the case of open-source botnets, the employed defensive measures are hardly sophisticated and are mostly self-developed. Sometimes, adaptations of standard mechanisms can be observed. Botnets made with construction kits typically either have the defensive measures integrated into the construction kit or make use of so-called defensive kits. This modular technique allows the integration of arbitrary defensive measures into the construction kit just before the malware binary is compiled. Depending on the sophistication of these defensive kits, they are either freely available or need to be purchased. Defensive measures for specialized botnets are normally a mixture of standard techniques along with custom-built developments that ensure the stealth properties of the malware binary.

Because security researchers actively study and circumvent these defensive mechanisms, the result is a constant arms race in which botnet operators and developers continually develop new and more advanced mechanisms which are then analyzed and bypassed by the security industry.

D. Deployment

Originally, malware spread by exploiting server services via portable disks, nowadays often USB sticks.

A new trend is the increasing exploitation of vulnerabilities in client-side applications. These are often ubiquitous on user desktops and thus an easy target. Examples for these kinds of applications are Adobe's Portable Document Format (PDF) reader and Flash, Microsoft Office programs, or Web browsers. The latter

can be exploited by so-called drive-by downloads on infected Web sites. These Web sites can be both legitimate sites hacked by criminals, or sites especially set up for the express purpose of infection. In the latter case, mass spam e-mails containing links to these sites lured users to these sites. According to the Websense 2010 threat report, 79.9 % of Web sites with malicious code were compromised legitimate sites [20].

Lately, there has been an increase in so-called targeted attacks which contain a social engineering component. Detailed background information is gathered on the intended targets and personalized messages are sent to the victims, either via e-mail or through social networking sites. By exploiting information about the target's current personal or professional situation (e. g. hobbies or work-related activities), the target can be tempted to open either infected attached files or visit suggested Web sites.

When open-source botnets are employed, the infection routines are generally self-developed or developed and shared within the community. When specialized botnets are used, the situation is similar, but for different reasons. Here, secrecy and often the environment in which the botnet is operating necessitate own developments. In construction kit-based botnets, infection vectors are usually supplied in the form of the already mentioned exploit kits.

The time required for the infection of hosts is difficult to estimate for all three classes of botnets. This also depends on the definition of "a sufficient number" of nodes which can be different for different purposes. When botnets are created for renting or selling them to third-parties [27], a common size of 10,000 hosts is bundled. For open-source and kit-based botnets, 10,000 hosts can often be infected within several hours to several days. In seldom cases, this can take more than a week. Specialized botnets often do not have the target of maximum infection speed as their purpose may not be financial gain but rather the accomplishment of long-term goals such as espionage. Thus, infection speed may not be of the utmost importance.

4. Resources Required for Tactical Countermeasures

Most of the common defensive techniques, such as firewalls, IDS, or anti-virus solutions, act on a local level. The locality is a problem when multiple targets are attacked that are managed by different entities, e. g. organizations with independent but cooperating branches. In addition, local measures can usually not prevent specific types of attacks, like DDoS attacks. A more sustainable and reliable way to counter such attacks is to conduct tactical countermeasures against the originating botnet.

In the following we will discuss the resources required to conduct different countermeasures that have the potential to take down the whole botnet. Two major types of countermeasures are considered. The first is classical countermeasures,

which are rather moderate in their implications, but are very limited because of their dependence on the cooperation of other organizations. The second type is more aggressive countermeasures with global consequences which can be conducted by a single organization and are therefore, more suitable for a tactical take-down.

Each of the presented countermeasures is discussed with regard to the resources money, human resources and skill-level, cross-domain expertise required by those, time for conducting the countermeasure, sustainability, and possible legal or ethical constraints. Since many factors influence the different resources, no hard numbers are given but rather important relationships and estimations are explained.

A. Classical Countermeasures

C&C Server Takedown
If the location of a C&C server has been determined, it can theoretically be shut down or disconnected. This can be made difficult if redundant infrastructures spread multiple instances of the server all over the world, in particular hosting them with different providers. In addition to the main C&C endpoint(s), backup channels have to be identified, if the takedown is to be sustainable. If this has been achieved, sustainability is usually very high, especially for kit-based botnets for which details about the infrastructure are either freely available or can be purchased from security companies or malware intelligence (e. g. [28]). The same is true for open-source botnets, as source code analysis can easily reveal structural information. Specialized botnets, due to their stealthy nature, require significant effort in malware dissection by reverse engineering and forensics along with time and money to identify C&C endpoints and backup channels.

Besides the required skills and money, cross-domain challenges like organizing cooperation with Internet service providers and local law enforcement authorities need to be faced. In an ideal case, the required time is in the vicinity of one hour. However, if lengthy analysis is needed and actions have to be coordinated with law enforcement in different countries, the entire process could take several months, if it is possible at all.

Legal constraints in some countries prohibit or complicate the takedown of C&C servers, enabling so-called bulletproof hosting requiring law enforcement intervention. In some countries, authorities and ISPs are reluctant to cooperate with security researchers or other security authorities. This is well-known and taken advantage of by botnet operators. Some ISPs notify customers if a site is about to be taken down and botnet operators can move the C&C server to another provider or a different country entirely.

DNS-based Countermeasures
If the C&C infrastructure of the botnet is based on DNS, then a classical countermeasure is deregistration of those domains required by the botnet. This has

to be done in cooperation with the respective DNS registrars and was successful in several cases. A requirement for this countermeasure to be sustainable is that the botnet's C&C infrastructure relies solely on DNS mechanisms. If this requirement is met, DNS countermeasures are independent of the class of botnet, although C&C mechanisms tend to be more sophisticated in kit-based (Twitter-based selection of C&C server names in Torpig) and specialized (Kraken, Conficker) botnets.

Where money, skills and cross-domain knowledge is concerned, the main organizational challenge is the cooperation with the DNS registrars. These companies have no immediate benefit from such cooperation and often do so mainly because of the publicity effect. National and international law enforcement agencies also need to be coordinated with as there are legal issues to be considered. In the majority of cases, a court warrant needs to be obtained.

The time needed for this countermeasure to come into effect is affected by both the duration of the legal proceedings, i. e. to obtain the court warrant, and the time it takes for the DNS settings to be propagated to other servers. The latter can take from several minutes to several days, depending on the DNS time-to-live settings.

Already connected computers are not affected by this countermeasure; only newly connecting hosts performing a lookup receive the false information. Thus, the size of the botnet steadily decreases. The sustainability is very high.

B. Proactive Countermeasures

Beside the classical countermeasure, there are also more effective proactive countermeasures.

Response DDoS

If the locations of the C&C endpoints are known, a possibility is to launch a counter-DDoS attack to disable these endpoints. This is only possible if there is a single or limit number of C&C servers and would not work in a botnet relying on P2P infrastructure. A requirement for this is the availability of one or more machines for creating the traffic.

Financial resources are needed for the setup and operation of the traffic creation machines. This could, for example, be done by renting a competing botnet. According to [21], a DDoS botnet can be rented from 200 USD per 24 hours or 500 USD per month. Experiments conducted by an unnamed source have shown that a range of C&C servers can almost be shut down by DoS attacks from a single machine. This countermeasure is generally independent of the category of botnet being attacked. However, to determine the botnet's operating parameters, especially its C&C endpoints, can require extensive analysis. The resources in terms of skills, cross-domain activities and money required for this are comparable to those of the C&C server takedown described earlier.

The application of a counter-DDoS is possible practically instantly as soon as information about the C&C endpoints is available. However, the sustainability is negligible. The attacked botnet is disabled only as long as the counter-DDoS is executed. Also, the implications of launching an own DDoS attack need to be considered. It has to be ensured that legitimate services running in close proximity to the C&C endpoints are not adversely affected. In addition to that, DDoS attacks are illegal or even considered a hostile act in most countries.

Hack-Back
Another proactive countermeasure is hacking back, i.e. penetrating the C&C server and taking down the botnet from within. This requires the existence of a flaw in the C&C infrastructure which needs to be found and exploited. A team of highly skilled penetration specialists needs to be involved.

In open-source botnets, the C&C protocol can be easily discovered by analyzing the source code. Standard source code auditing tools can be used to find weaknesses in the code. Construction kit botnets are usually sold together with the C&C server, although it is typically in binary form. Therefore, reverse engineering and binary code auditing skills are required. For specialized botnets it can be very difficult to obtain information about the C&C server. It is sometimes possible when using standard components with known vulnerabilities, e.g. specific Web servers. In all cases, analysts are required who are able to think outside box and identify non-obvious relationships between botnet components. Kit-based and specialized botnets require the highest reverse engineering skills.

The time required for such a hack-back differs among the different botnet classes. Because of the multitude of available code analysis tools, open-source botnets can often be hacked in a matter of minutes if a sufficient number of vulnerabilities exists, otherwise it is a matter of days depending on the complexity of the code. More time is required for kit-based botnets, since reverse engineering is needed most of the time. Because the server binary is available, offline and local stress tests can be performed. A minimum of several days can be expected, although the required time is more likely along the order of magnitude of weeks. Hacking of specialized botnets is very difficult. First the protocol has to be reverse engineered and possible weaknesses need to be derived. At least several weeks are needed for this.

Once access to the C&C server has been gained, diverse valuable information can be discovered. The installation of a root kit allows the complete control of the server machine and might even result in greater privileges than even the botherders have. However, in most countries it is illegal to gain access to computer systems of others without their knowledge. From an ethical point of view, hacking back is effectively fighting fire with fire.

Infiltration/Manipulation
Another proactive countermeasure is the infiltration of a botnet which might lead to the botnet being manipulated and/or disabled from within. This requires an in-depth understanding of the botnet's architecture and C&C protocol.

The skills needed vary for the different categories of botnets. Standard protocols, e. g. IRC and HTTP, can be automatically extracted, but especially for kit-based and specialized botnets, extensive reverse engineering skills are essential. Also, botnet domain knowledge coupled with out-of-the-box thinking is necessary to determine non-standard protocols. Cross-domain expertise is needed to identify and exploit weaknesses in the C&C protocol or architectures. Related fields in this case are communication protocol design, structured auditing as well as cryptography. Nevertheless, some manipulation vectors for standard protocols are well-known and can often be applied.

In terms of financial expenditure, analysis and monitoring environments need to be designed and built. Some organizations receive up to 100,000 malware samples per day. An investigation for the use of standard communication protocols takes place within a sandbox which has a minimum analysis time of 2 minutes. This requires around 140 machines running in parallel. Employing some heuristics allows the analysis to stop early. In addition to that, machines for monitoring are needed. Their number depends on the number of infiltrated botnets. Examples for existing frameworks for monitoring botnets are [17, 29].

The time required to infiltrate a botnet is difficult to estimate. A prerequisite is that malware samples are available for analysis. Their collection can already be a time-consuming task, especially if server-side polymorphism is used. Gaining an in-depth understanding of the botnet and its structures is also necessary. In case of standard protocols with standard manipulation vectors, a tactical takedown can be accomplished within minutes. The infiltration of botnets with non-standard protocols and the corresponding analyses can take up to several weeks, in lucky cases several days.

The sustainability of botnet infiltration is typically very high, provided it is not pursued too aggressively. For example, the aggressive monitoring of Storm by researchers was obvious to the botnet operators. If manipulations are made on the C&C server, they can be detected most of the time. To be truly effective, sudden strikes are essential.

The legal aspects of botnet infiltration still need to be investigated. From an ethical point of view, only the botnet's operation is interfered with. However, third-party data might be obtained or manipulated as a consequence, especially if the C&C is hosted on a hijacked system and depending on the architecture.

BGP Blackholing
Another possibility is the redirecting of botnet-related traffic, so-called sinkholing. The redirected traffic can simply be discarded or analyzed further to gather more information about infected machines. Resources with regard to money, skills and cross-domain knowledge are similar to those of regular C&C server takedowns. The processes can mostly be fully automated. However, the existence of backup channels for C&C processes can be challenging. Once sufficient information about the botnet and its structures is available, the C&C endpoints can be inserted into BGP feeds within a few seconds, although their propagation can take several minutes.

5. Summary and Outlook

In this paper we have discussed the resources required for setting up and taking down botnets. In order to structure this we have categorized botnets into three groups: completely open-source botnets or those that use open-source components, construction kit-based botnets which are normally for sale, and specialized botnets tailored to a very specific task.

In general, kit-based botnets are the easiest to setup and operate since they were designed with user-friendliness in mind. When setting up an open-source botnet, basic software development skills are required which can be obtained in a matter of hours or days. Challenges can often be overcome by taking advantage of community support. This community support is missing for specialized botnets, often due to secrecy requirements.

Classical countermeasures are often inadequate when faced with intricate botnet structures and protocols. Proactive countermeasures are much better suited to deal with the botnet threat. Sufficient funds, time and development expertise in the area of malware analysis and reverse engineering are the most important requirements. There is an increase in the amount of the respective required resources from open-source botnets through kit-based botnets to the specialized variants.

Currently, botnet operators are ahead in the arms race with security researchers, the anti-virus industry and law enforcement agencies. The currently performed anti-botnet activities are not as aggressive as they could be. This is partially due to lack of resources, the fear of legal consequences or uncoordinated efforts but also sometimes because of the fear of an intensifying arms race. Another reason is that monetary losses in the often targeted financial industry are still relatively moderate.

However, studies show that there is a steady increase in the amounts lost due to credit card fraud, extortion and other botnet-related crimes. Thus, with a corresponding increase in funds for anti-botnet activities, it stands to reason that there will be more offensive botnet takedown attempts in the not-too-distant future, despite the fact that this would spark the feared arms race.

REFERENCES

Symantec. Press release. Available online: http://www.symantec.com/about/news/release/article.jsp?prid=20090910_01, accessed February 2011.

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

Shadowserver. *60-Day Virus-Stats*. Available online: http://www.shadowserver.org/wiki/pmwiki.php/Stats/Virus60-DayStats, accessed February 2011.

F. Leder, T. Werner, P. Martini. *Proactive Botnet Countermeasures – An Offensive Approach*. In: C. Czosseck, K. Geers (Eds.), "The Virtual Battlefield: Perspectives on Cyber Warfare", IOS Press, 2009.

G. Klein, F. Leder, "Latest trends in botnet development and defense", Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2010.

Metasploit - Penetration Testing Resources. Available online: http://www.metasploit.com, accessed February 2011.

OpenSSL: The Open-Source Toolkit for SSL/TLS. Available online: http://www.openssl.org, accessed February 2011.

R. L. Rivest et al. *The MD6 hash function – A proposal to NIST for SHA-3*. Technical Report. Massachusetts Institute of Technology, Cambridge, MA, USA, April 2009.

J. Gailly, M. Adler. *zlib Compression Library*. Available online: http://www.zlib.net, accessed November 2010.

D. Fisher. *Storm, Nugache lead dangerous new botnet barrage*. Available online: http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1286808,00.html, accessed December 2010.

VMProtect homepage. Available online: http://vmpsoft.com, accessed November 2010.

N. Villeneuve. *Tracking GhostNet: Investigating a Cyber Espionage Network*. Available online: http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network, accessed February 2011.

N. Falliere, L. O. Murchu, E. Chien. *W32.Stuxnet Dossier*. November 2010. Available online: http://www.symantec.com/content/en/us/enterprise/

media/security_response/whitepapers/w32_stuxnet_dossier.pdf, accessed February 2011.

PC Plus. *Botnets Explained*. Available online: http://pcplus.techradar.com/feature/features/botnets-explained-30-09-10, accessed November 2010.

Stevens, K., Jackson, D. *ZeuS Banking Trojan Report*. Available online: http://www.secureworks.com/research/threats/zeus, accessed December 2010.

M86 Security Labs. *Web Exploits: There's an App for That*. Technical Report. Available online: http://www.m86security.com/documents/pdfs/security_labs/m86_web_exploits_report.pdf, accessed November 2010.

Marco Cremonini and Marco Riccardi. *The Dorothy Project: An Open Botnet Analysis Framework for Automatic Tracking and Activity Visualization*. In *Proceedings of the 2009 European Conference on Computer Network Defense* (EC2ND '09). IEEE Computer Society, Washington, DC, USA, 52-54

Kleissner, P. *AV Tracker homepage*. Available online: http://www.avtracker.info, accessed November 2010.

Higgins, K. J. *Zeus Attackers Deploy Honeypot Against Researchers, Competitors*. Available online: http://www.darkreading.com/insider-threat/167801100/security/attacks-breaches/228200070/index.html, accessed December 2010.

Websense, Inc. *Websense 2010 Threat Report*. Technical Report. Available online: http://www.websense.com/content/threat-report-2010-introduction.aspx, accessed November 2010.

Damballa. *Want to rent an 80-120k DDoS Botnet?*. Available online: http://blog.damballa.com/?p=330, accessed February 2011.

M. Bailey, E. Cooke, F. Jahanian, Y. Xu, and M. Karir. *A survey of botnet technology and defenses*. In Proceedings of the 2009 Cybersecurity Applications & Technology Conference for Homeland Security, pages 299–304, Washington, DC, USA, 2009. IEEE Computer Society.

P. Bächer, T. Holz, M. Kötter, and G. Wicherski. *Know your enemy: Tracking botnets*. Honeynet Project KYE series, 2007.

F. Leder and T.Werner. *Don't do this at home - owning botnets*. In T2 information security conference, Helsinki, Finland, 2009.

McAfee, Whitepaper, *Global Energy Cyberattacks: "Night Dragon"*, Version 1.4, February 10, 2011, http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf , accessed February 2011

D. Fisher. *Storm, nugache lead dangerous new botnet barrage*. http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1286808,00.html, accessed February 2011

Spencer Kelly, BBC, *Gaining access to a hacker's world*, 13 March, 2009, http://news.bbc.co.uk/2/hi/programmes /click_online/7938201.stm , accessed February 2011

Abuse.ch, *Zeus Tracker*, https://zeustracker.abuse.ch/ , accessed February 2011

G. Wicherski, *botsnoopd - Efficiently Spying on Botnets*, GovCert Symposium, September 16, 2008, Rotterdam, NL

PUBLICATION IV: ESTONIA AFTER THE 2007 CYBER ATTACKS: LEGAL, STRATEGIC AND ORGANIZATIONAL CHANGES IN CYBER SECURITY

Christian Czosseck, Rain Ottis and Anna-Maria Talihärm

Proceedings of the 10th European Conference on Information Warfare and Security, Tallinn, Estonia 7-8 July 2011, pp. 57-64.

Reprinted in 2011 in the Journal of Cyber Warfare and Terrorism, Vol 1, Issue 1.

ISBN: 978-1908272065
respectively
ISSN: 1947-3435

Abstract: At the time of the state-wide cyber attacks in 2007, Estonia was one of the most developed nations in Europe regarding the ubiquitous use of information and communication technology (ICT) in all aspects of the society. Relaying on the Internet for conducting a wide range of business transactions was and still is common practice. Some of the relevant indicators include: 99% of all banking done via electronic means, over a hundred public e-services available and the first online parliamentary elections in the world. But naturally, the more a society depends on ICT, the more it becomes vulnerable to cyber attacks.

Unlike other research on the Estonian incident, this case study shall not focus on the analysis of the events themselves. Instead it looks at Estonia's cyber security policy and subsequent changes made in response to the cyber attacks hitting Estonia in 2007. As such, the paper provides a comprehensive overview of the strategic, legal and organisational changes based on lessons learned by Estonia after the 2007 cyber attacks. The analysis provided herein is based on a review of national security governing strategies, changes in the Estonia's legal framework and organisations with direct impact on cyber security.

The paper discusses six important lessons learned and manifested in actual changes: each followed by a set of cyber security policy recommendations appealing to national security analysts as well as nation states developing their own cyber security strategy.

Keywords: Estonia, cyber attacks, lessons learned, strategy, legal framework, organisational changes

Disclaimer
The opinions expressed here are those of the authors and should not be considered as the official policy of the Cooperative Cyber Defence Centre of Excellence or NATO.

1. Introduction

Over three weeks in the spring of 2007, Estonia was hit by a series of politically motivated cyber attacks. Web defacements carrying political messages targeted websites of political parties, and governmental and commercial organisations suffered from different forms of denial of service or distributed denial of service (DDoS) attacks. Among the targets were Estonian governmental agencies and

services, schools, banks, Internet Service Providers (ISPs), as well as media channels and private web sites (Evron, 2008; Tikk, Kaska, & Vihul, 2010).

Estonian government's decision to move a Soviet memorial of the World War II from its previous location in central Tallinn to a military cemetery triggered street riots in Estonia, violence against the Estonian Ambassador in Moscow, indirect economic sanctions by Russia, as well as a campaign of politically motivated cyber attacks against Estonian (Ottis, 2008). By April 28th the cyber attacks against Estonia were officially recognized as being more than just random criminal acts (Kash, 2008). The details of the weeks that followed are described in (Tikk, Kaska, & Vihul, 2010).

The methods used in this incident were not really new. However, considering Estonia's small size and high reliance on information systems, the attacks posed a significant threat. Estonia *did not* consider the event as an armed attack and thus refrained from requesting NATO's support under Art. 5 of the NATO Treaty; instead, the attacks were simply regarded as individual cyber crimes (Nazario, 2007; Tikk, Kaska, & Vihul, 2010) or "ackitivism" as established by a well-known information security analyst Dorothy Denning (Denning, 2001). A further discussion on whether or not the 2007 attacks were an armed attack is beyond the scope of this paper. Many defence and security analysts have covered this particular topic and discussed e.g. the "juridical notion of information warfare" (Hyacinthe, 2009), a "taxonomies of lethal information technologies" (Hyacinthe & Fleurantin, 2007), formulated a "Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict" (Brown, 2006), or "legal limitations of information warfare" (Ellis, 2006).

The incident quickly drew worldwide attention, and media labelled the attacks the first "Cyber War" (Landler & Markoff, 2007). This led to an overall "Cyber war hype" that was continuously carried forward by media, researchers and policymakers. This exaggerating rhetoric was employed during following conflicts like Georgia 2008 or Kyrgyzstan 2009, and such misuse of terminology has already received a fair amount of criticism (Farivar, 2009).

The 2007 attacks have shown that cyber attacks are not limited to single institutions, but can evolve to a level threatening national security. Looking back, the Estonian state was not seriously affected since to a larger extent state functions and objects of critical information infrastructure were not interrupted or disturbed (Odrats, 2007). However, nation states did receive a wake-up call on the new threats emerging from cyber space, alongside with new types of opponents.

The following three sections will provide a comprehensive overview of major changes in Estonia's national cyber security landscape, namely the changes of national policy. As a result, several laws and regulations were introduced, while others were amended, and there were several changes in the organisational landscape.

This paper features six lessons learned that were identified as most remarkable in the case study of Estonia. It concludes with several strategic cyber security recommendations.

2. Development of national strategies

The benefits as well as threats of the use of Internet-related applications to information societies are identified by a number of Estonian high level policies and strategies.

The *Estonian Information Society Strategy 2013* (MoEAC, 2006), in force since January 2007, promotes the broad use of ICT for the development of a knowledge-based society and economy. Given that cyber attacks on a scale matching that of Estonia in 2007 were unseen and likely unpredicted so far, it is not surprising that the risk of massive cyber attacks was not taken into serious consideration in the strategy – nor in other national policy documents from that era (see e.g. the implementation plan of the Information Society Strategy for 2007-2008, MoEAC, 2007).

The *National Security Concept* of Estonia published in 2004 (MoD, 2004) and the government's action plan in force at this time (Estonian Government, 2007) were no exception since these documents did not even mention possible cyber threats or related actions.

It was only after the 2007 cyber attacks that cyber security instantly found its way into the national security spotlight.

2.1 Policy and strategy responses since 2007

In July 2007, shortly following the cyber attacks, the Government approved the *Action Plan to Fight Cyber-attacks (Kaska, Talihärm, & Tikk, 2010)*. In September 2007, the revised Implementation Plan 2007-2008 of the Estonian Information Society Strategy 2013 (MoEAC, 2007) was approved. The document holds a generic statement that critical information infrastructure should be developed in such a way that it operates smoothly in "emergency situations" (MoI 2009).

Cyber Security Strategy
In May 2008, the Estonian government adopted the newly drafted *Cyber Security Strategy (CSS)* as a comprehensive policy response to the cyber attacks. The strategy was prepared by a multi-stakeholder committee including relevant ministries, agencies and private sector representatives.

The *CSS* considers cyber security a national effort responding to the asymmetric threat posed by cyber attacks. The strategy underlines that state-wide cyber security

requires active international cooperation and the promotion of global responses. On a national level, the strategy suggests implementing organisational, technical and legal changes. Further, it aims at developing an over-arching and sophisticated *cyber security culture* (MoD, 2008).

Based on a post-attack assessment of the situation in Estonia, the CSS identified five strategic objectives:

1. The development and large-scale implementation of a system of security measures;
2. Increasing competence in cyber security;
3. Improvement of the legal framework for supporting cyber security;
4. Bolstering international cooperation; and
5. Raising awareness on cyber security.

In May 2009, the CSS implementation plan for the 2009-2011 cycle was adopted by the government. The plan called for concrete actions in five priority areas and became the main source for the comprehensive cyber security approach in Estonia (Estonian Government, 2009).

National Security Concept

The *National Security Concept*, which was updated and approved in May 2010, represents Estonian government's second major cyber security policy response. It recognizes Estonia's growing reliance on ICT along with the increasing threat posed by terrorists and organised crime groups. Cyber crime should receive special attention, and solutions are to be found in co-operation between agencies on both national and international level. Cyber security shall be ensured by "[...] reducing vulnerabilities of critical information systems and data communication connections" Critical systems shall stay operational, even if the connection to foreign countries is temporarily malfunctioning or has ceased to function. To support these actions, the necessary legislation should be developed and public awareness raised (MoD, 2010).

The National Security Concept led to the revised *Guidelines for Development of Criminal Policy until 2018,* published in October 2010. The Police shall focus on preventing the spread of malware and the growing number of "hacking" incidents. Furthermore "[t]he existence of a sufficient number of IT specialists in law enforcement agencies shall be ensured in order to set bounds to cyber crime more efficiently." (MoJ, 2010). Other strategies like the *Estonian Information Society Strategy 2007-2013* have received only minor cyber security related amendments.

In addition, since the 2007 attacks, Estonia has become one of the major advocates of cyber security on the international level. As one result, NATO initiated the development of a unified strategy against cyber attacks (Blomfield, 2007) and in 2010 NATO adopted the new strategic concept that recognizes cyber attacks as a threat to the alliance and opts for the enhancement of alliance's and nations' capabilities to face the threat (NATO, 2010).

Moreover, Estonia has actively supported a number of international organisations such as the Council of Europe in its fight against cyber crime (MoFA, 2010a), Association of Southeast Asian Nations in promoting the harmonization of laws concerning cyber crime (MoFA, 2010b) and United Nations in contributing an expert to the task force on *Developments in Information and Communication Technology in the Context of International Security* (MoFA, 2010c).

3. Development in the legal field

The 2007 attacks prompted major changles in the Estonian legislative landscape and in some cases enhanced the changes already underway. Legal amendments involved several areas of law related to cyber security (see Table 1): criminal law (including aspects of criminal procedure) and crisis management law. The Estonian incident did not, however, directly touch upon the legal regime applicable to armed conflicts since the attacks were treated by national authorities as acts of crime.

Other laws such as the Electronic Communications Act were also updated but did not involve considerable changes in the context of cyber security (Estonian Government, 2010).

Table 1.(Kaska, Talihärm, & Tikk, 2010)

Constitutional law				
Fundamental rights and freedoms; Organisation of the state; Execution of public authority				
Private law	**Public administrative law**	**Criminal law**	**Crisis management law**	**War-time law / national defence law**
Information society services	General administrative procedure law supporting the accessibility of information society	Substantive criminal law	Critical infrastructure protection (CIP)	National defence organisation
eComms infrastructure provision	Availability of public information and public e-services	Criminal procedure law	Critical information infrastructure protection (CIIP)	National defence in peacetime
Provision of eComms services to end users	Data processing and data protection	International cooperation		National defence in conflict/ wartime
General private law supporting the functioning of information society (eCommerce, digital signatures)				

3.1 Penal Code

Mostly due to the need to harmonize the Estonian Penal Code with the *Council of Europe Convention on Cyber Crime* (Council of Europe, 2001) and the Council Framework Decision 2005/222/JHA of on attacks against information systems (Council of Europe, 2005) all cyber crime related provisions in the Penal Code were reviewed. The amendments targeted the provisions addressing attacks against computer systems and data, widened the scope of specific computer crime provisions (e.g. criminalizing the dissemination of spyware and malware), added a new offence of the preparation of cyber crimes, modified the provision concerning acts of terrorism and filled an important gap (Estonian Government, n d) in the Penal Code by enabling differentiation between cyber attacks against critical infrastructure (with the purpose of seriously interfering with or destroying the economic or social structure of the state) and ordinary computer crime (MoI, 2009).

3.2 Amendments Relevant to Criminal Procedure Law

The amendments in the Penal Code resulted partly from the regulatory limitations that arose in relation to the application of the Code of Criminal Procedure (CCP) to the 2007 attacks (MoJ, 2010b) as CCP §§ 110-112 maintain that evidence may be collected by surveillance activities in a criminal proceeding if the collection of evidence is a) precluded or especially complicated and b) the criminal offence under investigation is, at the minimum, an intentionally committed crime for which the law prescribes a punishment of at least three years' imprisonment (MoJ, 2010b). However, during the Estonian attacks in 2007 it became apparent that almost none of the committed offences met the threshold of "three years" imprisonment and that precluded the employment of surveillance measures (Estonian Government, 2007b). Therefore, the changes in the Penal Code prescribed higher maximum punishments and also corporate liability for cyber crime offences.

3.3 New Emergency Act

The new Emergency Act (EA) (MoI, 2009) was adopted in June 2009 and reviewed the current setup of national emergency preparedness and emergency management structure, including the responses to cyber threats.

Offering a comprehensive approach, the act foresees a system of measures which include preventing emergencies, preparing for emergencies, responding to emergencies and mitigating the consequences of emergencies ("crisis management" (MoI, n d). It is the providers of public services and information infrastructure owners that are tasked with everyday emergency prevention and ensuring the stable level of service continuity. Providers of vital services are obliged, among other assignments, to prepare and present a continuous operation

risk assessment (EA §38) and an operation plan (EA §39) to notify the citizens about events significantly disturbing service continuity as well as to provide the necessary information to supervisory bodies. In addition to the above, there are certain provisions that specifically address threats against information systems, such as an obligation for the providers of vital services to guarantee the smooth application of security measures in information systems and information assets used for the provision of vital services.

4. Development of organisations

Before the 2007 cyber attacks Estonia had relatively few organisations dedicated to (national) cyber defence. Since then, Estonia has made some key organisational changes to better deal with the cyber threats. The most significant ones are described below.

A high level organisational change was the formation of the *Cyber Security Council* under the Government Security Committee, a body foreseen by the National Cyber Security Strategy. The Council reports directly to the Government Security Committee and is therefore well-placed for coordinating inter-agency and international cyber incident response.

4.1 EIC, CERT-EE and CIIP

Estonian Informatics Centre (EIC) is a state agency that is responsible for managing and developing public information services and systems (MoEAC, 2009). It is also tasked with providing cyber security for these services and systems. Even though a national CERT had been established in 2006 as a department of the EIC, its capabilities and experience were still quite modest at the time of the attacks. In 2009, as a result of the National Cyber Security Strategy, the Department of Critical Information Infrastructure Protection (CIIP) was added to the structure of EIC, in addition to the already existing CERT. The main tasks of the new department include supervising risk analyses of critical information infrastructures and developing protective measures.

4.2 Cyber Defence League

During the cyber attack campaign, the Estonian CERT was assisted by an informal network of volunteer cyber security experts. This provided much needed additional capabilities, such as increased situational awareness, analysis capability, quick sharing of defensive techniques between targeted entities, as well as an extended network of direct contacts to international partners.

The roots of this informal group derive from the late 1990ies, when Estonia was adopting a national ID card system. Over the years, the network of professionals had also cooperated against criminally motivated cyber attacks targeting critical infrastructures (e.g., Estonian banks). A later development was the formalisation of this loose cooperation into the Cyber Defence League (CDL) in 2009. The Defence League is a volunteer national defence organization in the military chain of command. The CDL is part of the Defence League and unites cyber security specialists who are willing to contribute their time and skills for the protection of the high-tech way of life in Estonia, especially assisting the defence of critical information infrastructure. It is important to note that this is a defensive organisation, not designed to harass political adversaries in (anonymous) cyber attack campaigns. In January 2011, the CDL was reorganized into the Cyber Defence Unit of the Defence League, but the CDL name is still widely used.

CDL's key activities include organizing training and awareness events, as well as cyber defence exercises. In 2010, the CDL was involved with the Baltic Cyber Shield exercise organised by Cooperative Cyber Defence Centre of Excellence (Geers, 2010), the US-led International Cyber Defence Workshop, as well as a series of national exercises. The CDL is a good example of managing in a productive manner the expertise and enthusiasm of motivated cyber security specialists.

5. Six recommendations

Given that the major changes have been discussed above, the next section will feature six significant lessons learned from the 2007 cyber attacks against Estonia:

5.1 Comprehensive strategy approach

It is evident that Estonia has taken into account the lessons learned from the 2007 incident, the most significant step being the quick establishment of a comprehensive policy response which has led to the adoption and subsequent implementation of the national Cyber Security Strategy. The Estonian example emphasises the need for nation-wide cooperation and countermeasures against cyber crime, involving major stakeholders of the public and private sector.

It remains to be debated whether cyber security should be handled in a single comprehensive strategy or form a sub-section of all other relevant strategies touching upon ICT. However, considering the speed of technological advancements and comparing it with the speed of developing national strategies, the Estonian approach of having a single strategy might be the one more advisable.

The 2007 attacks triggered the cyber security strategy drafting in Estonia. However, countries should not wait for such triggers and should pro-actively conduct

a thorough and comprehensive risk assessment of their cyber infrastructure. Furthermore, often only the context and additional information will reveal if the attack was launched with crime, espionage, terrorism or military motivation. Therefore, close cooperation between relevant agencies remains a *sine qua non* to success in this arena.

5.2 Politically Motivated Cyber Attacks

Another aspect to consider is the shift of attention in terms of cyber security threats over the last decade. While the first half of the decade the cyber security focus was on criminal and espionage attacks (if recognised as a national security issue at all), the second half witnessed a surge in politically motivated cyber attacks (Nazario, 2009). The significance of this development is that targets have transformed. A politically motivated attacker is likely to attack visible and politically significant targets (such as the public website of a government agency or a company that has angered an interest group), which are of little interest to criminals and intelligence agencies. This shift in targets requires everyone to reassess their risks and security requirements.

Politically motivated actors can cover the entire spectrum of cyber attack, from high-profile strikes against critical infrastructure, to millions of pinprick attacks that can weaken the state over a long period of time (Lemay, Fernandeza, & Knight, 2010; Liles, 2010; Ottis, 2009). As the threat of politically motivated attacks threatening national security is not likely to go away in the foreseeable future, it must be addressed as a national security issue in order to get the full attention of policymakers.

5.3 Legal Recommendations

An analysis of the Estonian legal order governing the domain of information society underlines that a secure information society needs to be comprehensively supported by norms involving several legal disciplines. The broad approach illustrated by the Estonian legal framework brings together the areas of private and public law, and completes the spectrum of cyber incident regulation by engaging criminal law, crisis management regulation and wartime law/national defence legal order. It is vital for countries to realize that the international cyber security regulation involves a wide range of legal areas and the review of relevant regulatory frameworks and the identification of possible uncovered "grey areas" is highly recommended.

Within national legal systems, a review of criminal law (penal law) appears to be a central issue. Attacks against critical (information) infrastructure, politically motivated cyber attacks, possible cases of cyber terrorism, as well as related provisions for investigation and prosecution, should all be reflected in the domestic

criminal law or other national acts. Broad and inclusive national implementation of the *Council of Europe Convention on Cybercrime* is of crucial importance, especially considering the cross-border nature of cyber crime.

Additionally, the Estonian experience underlined the need to establish common security standards for all computer users, information systems and critical infrastructure companies (MoD, 2008). By 2011, steps have been taken to establish such standards for service providers within the framework of the Electronic Communications Act, but more detailed rules for end-users' conduct and/or legal obligations are still needed.

5.4 Exercises and Education for the Masses

A key component of enhancing (national) cyber security is cyber security awareness and education. This should not be limited to professionals in governmental or private institutions, but must cover the whole spectrum from a citizen using ICT for everyday things to senior policy makers, considering the skills and knowledge needed at every level. This includes law enforcement agencies and especially the judicial system that has a central role in interpreting the regulatory aspects of cyber security. By developing different solutions well suited for each groups, a *broad and sophisticated cyber security culture* can be implemented, as aimed for in the CSS.

Estonia recognized its lack of sufficient number of well-trained information security experts and developed a new Master's program for Cyber Security *S*tudies in 2008. The *Cyber Defence League* is another venue for actively training experts in cyber security. Further measures, such as information campaigns for the secure use of the Internet, special classes in high school or vocational training should be considered by Estonia and other nation states.

Additionally, cyber security exercises organised both on national and international level serve as effective preparation to respond to cyber attacks. Exercises like *Cyber Europe 2010* (ENISA, 2010) require efficient coordination between agencies and private shareholders and should be regularly conducted.

5.5 International Relations

The attacks against Estonia in 2007 underlined the importance of international cooperation as it became even more apparent that in the context of responding to cyber threats, one country can do little alone. To that end, active participation in the work of major organizations dealing with cyber security requires keeping national developments and legal framework up to date and serves as a useful ground for new initiatives, further collaboration and regional or global forum. Moreover, the

ratification of instruments such as the Council of Europe Convention of Cyber Crime that aim to harmonise cyber crime regulation worldwide should be supported and promoted.

Beside the political will for cooperation, national multi- and bilateral agreements, information sharing agreements, cooperation of law enforcement agencies, joint investigation teams, international exercises, formal and informal networks and other international initiatives are vital for effective prosecution and investigation of cyber crime offences.

5.6 Harnessing the Volunteers

It is well known that most of the Internet infrastructure is owned and operated by the private sector. It follows that there is a pool of experts in the private sector, who could provide a meaningful contribution to national cyber security, regardless of their actual position in the private sector. This also includes experts in the public sector, who do not work in their area of expertise.

Clearly, there are limits to the use of volunteers, whether their potential role is in offensive or defensive activities (Ottis, 2009). However, if proper legal, policy and operational frameworks are in place, volunteers can significantly increase national cyber security capability.

6. Conclusions

While in hindsight, the cyber attacks against Estonia were not as severe as often referred to, they still triggered an understanding of threats from cyber space as threats potentially affecting national security and prompted a wake-up call concerning the risks associated with the "careless use"of digital information technologies (e.g., Internet). For instance, the risk posed by politically motivated individuals should be regarded as a possible element of a serious threat to cyber security.

By reviewing the strategic, legal and organisational changes that Estonia has undergone after the 2007 cyber attacks, this paper provides a concise list of key changes that have taken place on the legislative and administrative levels. While this paper describes some new assets that so far appear to be unique to Estonia, such as the formation of the Cyber Defence League, it offers several recommendations to national security planners performing beyond Estonia's national boundaries.

Many of the aforementioned recommendations are not new; but they have passed a practical test through the real-life Estonian case study. Accordingly, these recommendations are more than a set of purely theoretical proposals.

Lastly, based on the foregoing analysis, it is important to stress the fact that cyber security of a nation state can only be achieved by an interlocked approach covering national policies, its legal framework and organisations involving both public and private actors, as well as necessary changes identified by a realistic risk assessment.

ACKNOWLEDGEMENT

We would like Mrs. Kadri Kaska and the unknown reviewer for their substantial comments they provided us with in the course of writing this paper.

REFERENCES

Blomfield, A. (2007). Estonia calls for Nato cyber-terrorism strategy. Retrieved from http://www.telegraph.co.uk/news/worldnews/1551963/Estonia-calls-for-Nato-cyber-terrorism-strategy.html.

Brown, D. (2006) "A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict" *Harvard International Law Journal,* 47 (1), 179-221.

CDL. (n.d.). Cyber Defence League. Retrieved from http://www.kaitseliit.ee/index.php?op=body&cat_id=395.

Council of Europe. (2001). Convention on Cybercrime. Retrieved from http://conventions.coe.int/treaty/en/treaties/html/185.htm.

Council of Europe. (2005). Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. *Official Journal L 69*, 67-71.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy. *Networks and netwars: The future of terror, crime, and militancy*, 239–288.

Ellis, B. (2001) "The International Legal Implications and Limitations of Information Warfare: What Are Our Options?". Retrieved Mar. 2, 2011 from http://www.iwar.org.uk/law/resources/iwlaw/Ellis_B_W_01.pdf.

ENISA. (2010). EU Cyber Security Exercise 'Cyber Europe 2010'. Retrieved January 31, 2011, from http://www.enisa.europa.eu/media/press-releases/cyber-europe-20102019-cyber-security-exercise-with-320-2018incidents2019-successfully-concluded.

Estonian Government. (2007a). Programme of the Coalition for 2007-2011.

Estonian Government. (2007b). Explanatory Memorandum to the Draft Act on the Amendment of the Penal Code (116 SE) (In Estonian). Retrieved from http://www.riigikogu.ee/?page=pub_file&op=emsplain&content_type=application/msword&u=20090902161440&file_id=198499&file_name=KarS seletuskiri (167).doc&file_sise=66048&mnsensk=166+SE&etapp=03.12.2007&fd=29.10.2008.

Estonian Government. (2009). Valitsus kiitis heaks küberjulgeoleku strateegia rakendusplaani aastateks 2009–2011. Retrieved from http://uudisvoog.postimees.ee/?DATE=20090514&ID=204872.

Estonian Government. (2010). Explanatory Memorandum to the Act amending the Electronic Communications Act (424 SE) (In Estonian). Retrieved from http://www.riigikogu.ee/?page=pub_file&op=emsplain&content_type=application/msword&file_id=535868&file_name=elektroonilise side muutmine seletuskiri (424).doc&file_size=31650&mnsensk=424+SE&fd=.

Evron, G. (2008). Battling botnets and online mobs: Estonia's defense efforts during the internet war. *Georgetown Journal of International Affairs*, *9*(1), 121–126.

Farivar, C. (2009). A Brief Examination of Media Coverage of Cyberattacks (2007 - Present). In C. Czosseck & K. Geers (Eds.), *The Virtual Battlefield: Perspectives on Cyber warfare* (pp. 182 - 188). IOS Press.

Geers, K. (2010). Live Fire Exercise: Preparing for Cyber War. *Journal of Homeland Security and Emergency Management*, *7*(1).

Hyacinthe, B. (2009). *Cyber Warriors at War*. Xlibris, pp. 82-85.

Hyacinthe, B. & Fleurantin, L. (2007). Initial supports to regulate information warfare's potentially lethal information technologies and techniques. *Proceedings of the 3rd International Conference on Information Warfare and Security* (pp. 206-207). Academic Conferences Limited.

Kash, W. (2008). Lessons from the cyberattacks on Estonia. Retrieved from http://gcn.com/articles/2008/06/13/lauri-almann--lessons-from-the-cyberattacks-on-estonia.aspx.

Kaska, K., Talihärm, A.-M., & Tikk, E. (2010). Building a Comprehensive Approach to Cyber Security. CCD COE Publications.

Landler, M., & Markoff, J. (2007). In Estonia, what may be the first war in cyberspace. *The New York Times*. Retrieved from http://www.nytimes.com/2007/05/28/business/worldbusiness/28iht-cyberwar.4.5901141.html.

Lemay, A., Fernandeza, J. M., & Knight, S. (2010). Pinprick attacks, a lesser included case? In C. Czosseck & K. Podins (Eds.), *Conference on Cyber Conflict Proceedings* (pp. 183 - 194). Tallinn: CCD COE Publications.

Liles, S. (2010). Cyber Warfare: As a form of low-intensity conflict and insurgency. In C. Czosseck & K. Podins (Eds.), *Conference on Cyber Conflict Proceedings* (pp. 47 - 57). Tallinn: CCD COE Publications.

MoD. (2004). National Security Concept of the Republic of Estonia.

MoD. (2008). Cyber Security Strategy. Retrieved from http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf.

MoD. (2010). NATIONAL SECURITY CONCEPT. Retrieved from http://www.kmin.ee/files/kmin/nodes/9470_National_Security_Concept_of_Estonia.pdf.

MoEAC. (2006). Estonian Information Society Strategy 2013. Retrieved from http://www.riso.ee/en/system/files/Estonian Information Society Strategy 2013.pdf.

MoEAC. (2007). Implementation Plan 2007-2008 of the Estonian Information Society Strategy.

MoEAC. (2009). Statute for the Development of National Information System (in Estonian). Retrieved from https://www.riigiteataja.ee/akt/13219897.

MoFA. (2010a). Estonia Supports Council of Europe in Fight Against Cyber Crime. Retrieved from http://www.vm.ee/?q=en/node/9315.

MoFA. (2010b). Foreign Minister Paet Invited EU and Southeast Asian Nations to Co-operate in Backing Cyber Defence. Retrieved from http://www.vm.ee/?q=en/node/9512.

MoFA. (2010c). National Experts Shared Cyber Security Recommendations with UN Secretary General. Retrieved from http://www.vm.ee/?q=en/node/9722.

MoI. (2009). Estonian Emergency Act (unofficial translation). Retrieved January 4, 2011, from http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XXXXX26&keel=en&pg=1&ptyyp=RT&tyyp=X&query=hadaolukorra.

MoI. (n.d.). Ministry of the Interior, Department of crisis management and rescue policy (in Estonian). Retrieved January 4, 2011, from http://www.siseministeerium.ee/elutahtsad-valdkonnad-ja-teenused-2.

MoJ. (2010a). Guidelines for Development of Criminal Policy until 2018. Retrieved from http://www.just.ee/arengusuunad2018.

MoJ. (2010b). Estonian Code of Criminal Procedure (unofficial translation). Retrieved from http://www.legaltext.ee/text/en/X60027K6.htm.

NATO. (2010). Strategic Concept for the Defence and Security of the Members of the NATO. Retrieved December 30, 2010, from http://www.nato.int/cps/en/natolive/official_texts_68580.htm.

Nazario, J. (2007). Estonian DDoS Attacks – A summary to date. Retrieved from http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/.

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

Odrats, I. (Ed.). (2007). *Information Technology in the Public Administration of Estonia Yearbook 2007*. Ministry of Economic Affairs and Communication.

Ottis, R. (2008). Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. *Proceedings of the 7th European Conference on Information Warfare* (p. 163). Academic Conferences Limited.

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

Tikk, E., Kaska, K., & Vihul, L. (2010). *International Cyber Incidents: Legal Considerations* (p. 130). Tallinn: CCD COE Publications.

PUBLICATION V: EVALUATION OF NATION-STATE LEVEL BOTNET MITIGATION STRATEGIES USING DEMATEL

Christian Czosseck

Proceedings of the 11th European Conference on Information Warfare and Security,
Laval, France 7-8 July 2012, pp. 94-103.

ISBN: 978-1-908272-55-3

Abstract: Botnets have been recognised as a possible threat to national security, and over recent years national cyber security thinkers have started to draft national level strategies to reduce the threat posed. The steady increase in the number of infected machines and the damage caused by botnet-mounted attacks shows that the success so far has been limited. This research analyses nation-state and inter-state level botnet defence and mitigation strategies and ultimately evaluates their impact on the botnet threat by employing the *Decision-Making Trial and Evaluation Laboratory* (DEMATEL) method on empirical data collected via interviews from experts in the field.
This paper develops and presents a system of nation-state level strategy groups and a simple model of effects they might have on the botnet threat. Based on this framework, the reciprocal influence of each element pair is identified, with the help of knowledgeable experts, and serves as the basis to conduct an analysis utilising the DEMATEL method.
As a result we present a model of the influence that these strategy groups have on the botnet threat, identify strongly and weakly influential elements in this system and present a ranking based on these findings. This will lead to a recommendation as to which is the preferred strategy.

Keywords: Botnets, DEMATEL, Cyber Defence, Strategy evaluation

Disclaimer
The opinions expressed here are those of the authors and should not be considered the official position of the NATO Cooperative Cyber Defence Centre of Excellence or NATO.

1. Introduction

Over recent years, cyber-crimes, and with them botnets in their sheer unlimited ways of usage, have risen from a primarily cyber-crime issue to nation-state security concerns. Besides "classical" spam and DDoS campaigns, executed for monetary gain, politically-motivated cyber-attacks, with botnets as their preferred means, are on a steady rise (Nazario, 2009). Users of botnets range from individuals and other organised groups up to nation-states (Ottis, 2010). Czosseck and Podins (2011) offer a generic taxonomy of users and usages of botnets based on recent history.

Under the lasting impression of the cyber-attacks against Estonia back in 2007, nation-states all over the world started to seriously recognise the cyber domain in

a nation-state security context, and with it the newly emerging threats including botnet-mounted attacks. The increasing number of dedicated national cyber-security strategies reflects this.

These nations have their national interests challenged on multiple frontlines. Cyber-crime is now an organised, highly professionalised business offering well-developed exploits and malware to anyone willing to pay, ultimately hurting the economy on a large scale. As an example, the damage of cyber-crime to the UK economy is estimated to be £27bn per annum (Cabinet Office UK & Detica Ltd., 2011). Besides this, the very same technology and knowledge about vulnerabilities is sold via lawful channels, especially in the context of services dedicated to nation-state customers such as law enforcement, military or intelligence services (GTISC & GTRI, 2011).

The responses to this development are manifold and reach from technical solutions at one end to governmental actions on both national and international scales at the other.

A system of strategic options available to a nation-state actor is introduced in Section 2, followed by simplified effect model in Section 3 of this paper. As an empirical basis for further analysis, knowledgeable experts are interviewed and their answers analysed with DEMATEL in Section 4, motivating the discussion and conclusions of this paper.

2. Nation-state level botnet mitigation strategies

This research focuses on the nation-state level strategies understood as those instruments normally initiated, introduced or supported by governments, either because they have the unique authority to do so or they are in the position to facilitate it on a nation-state scale. Examples include, but are not limited to, state policies, changes to national legal frameworks or international collaboration e.g. in the framework of existing international organisations.

In the following research a system of 10 strategy groups of similar strategies is developed, motivated by existing practice and academic research. In this context, similar means different strategies which result in a similar effect, target similar stakeholders or use similar methods. They are encouraged by the findings of the ENSIA Botnet Study (Plohmann *et al*., 2011) and other studies, especially those by Dunn (2005) and Eeten *et al*. (2010), as well as the analysis of current national strategies, or they reflect examples of existing or academically discussed actions taken.

2.1 Promotion of dedicated and coordinated R&D Programs

For cyber security to be developed effectively on a nation-state level, specialised and coordinated research becomes crucial. As Dunn (2005) argues, the fundamental issue and major challenge is the interdisciplinary nature of the research that needs to be conducted. While the existing research on IT-security is mainly technical by nature, this is not seen as enough to cover all aspects of the complex systems on hand, requiring a *"holistic and strategic threat and risk assessment at the physical, virtual and psychological level"*. Anderson *et al*. (2008) argues the same.

This group of strategies reflects approaches such as the development or promotion of nation-state research agendas, the support of these with special grants or programmes, or the development of new/ specialised curricula. In particular, by using instruments existing to govern the higher education system present in most nations, the availability of a specialised workforce can be positively affected.

2.2 Improvement of international law enforcement

Organised cyber-crime can be seen as the current root cause of the existing botnet threat. As the use of botnets for mostly criminal purposes is a highly lucrative business, a highly professionalised "underground economy" emerged. Botnet masters are highly motivated to make their investment resilient against takedowns and are actively exploiting grey areas in international legal frameworks, missing cooperation between nations or bullet-proof hosting opportunities. Taking down botnets nowadays mostly implies an internationally-coordinated, timely effort between different law enforcement groups.

This group of strategies includes examples such as the Council of Europe Cybercrime Convention (Council of Europe, 2001), showing that international treaties are one way to mitigate obstacles in international law enforcement cooperation. Agreements between nation-states, legislation or regulations within supranational organisations such as the EU, or commitments of or recommendations to nations under the umbrella of international organisations are other possibilities to harmonise the legal frameworks. This group includes actions to address the "IP addresses are private data" issue in the EU, exploring/implementing exceptions to criminal offences for certain stakeholders in order to ease the legal risks of becoming active (e.g. the "Good Samaritan Law", or exceptions from privacy concerns for IP exchange or reverse engineering of malware (breach of license issue), as encouraged in Plohmann *et al*. (2011).

2.3 End-user notification, support and good-behaviour incentives

As is commonly known and reflected in the findings of Eeten *et al*. (2010), infected end-users represent the largest part of the botnet population. There are

many reasons for this, including the lack of general IT-security awareness, the use of stolen (and sometimes manipulated) software or general weaknesses to social engineering-based attacks. Often end-users are not aware of the infection or are not capable or willing to disinfect.

To support end-users, a proper notification is required in the first place. Additionally, (negative) incentives for self-cleaning, such as the introduction of walled gardens on an ISP level, are ways to increase pressure on end-users to encourage good practices. As these means are not available for free and also pose the concrete risk of alienating customers, ISPs are often reluctant to implement such means.

This group of strategies firstly covers activities aimed at establishing a system for notifying end-users about a present infection, and to help them in the process of clearing the infection from their systems. The Cyber Clean Centre in Japan (CCC, 2011) and the German Anti-Botnet-Advisory Centre (ECO, 2011) are examples of initiatives in which a joint private/ public effort was made to assist end-users.

Secondly, governmental (e.g. legal) and successively ISP-based instruments to encourage good behaviour are included in this group. A government could support or enforce implementation of "walled gardens" by introducing appropriate laws. Another method is the introduction of national acts penalising end-user misbehaviour, threatening them with e.g. disconnection from the Internet and suspension of Internet usage for a longer period of time. This has been possible in France since 2009 (BBC, 2011), and is ultimately based on new EU legislation (European Comission, 2007).

2.4 ISP obligations and incentives to act

The empirical data presented and analysed in Eeten *et al.* (2010) highlights the central role ISPs are playing in the mitigation of botnets and their effects. They find that within the extended OECD, approximately 200 ISPs are covering about 80% of all Internet users, so governments are in a good position to tackle the problem by speaking to a relatively small group. However, they also identified that ISPs differ significantly with regards to the botnet activity within them, reflecting different security means applied by them.

This group of strategies reflects actions taken by nation-states to encourage ISPs to implement means and processes to pre-emptively mitigate botnet infections or their actions (beyond activities that directly target end-users). Service-based means, such as blocking port 25 as default for all retail customers, the implementation of network traffic monitoring and controlling, automatic botnet mitigation technology, as suggested by Asghari (2010), or the monitoring of traffic to well-known C&C servers are examples of additional actions which could be taken. There are various mechanisms for these, ranging from financial support or loans to active negotiations or regulations enforced by ISPs.

2.5 Awareness campaigns

Considering the increasing complexity of IT security threats and their mitigation solutions, it might be safe to assume that the general IT security awareness and the level of good behaviour is not on a adequate level to face the problem. Raising security awareness at all levels of society and explaining as well as encouraging the civic responsibility of everyone was identified as key by, for example, Plohmann *et al.* (2011). While related, this is different from end-user notification as it is a protective measure, helping to prevent an infection in the first place.

This group of strategies represents those measures taken to raise general public awareness on a broad and continuous basis, similar to campaigns for AIDS, smoking or drugs. This might include information portals dedicated to the user, as are present in many countries such as Germany (ECO, 2011) and Japan (CCC, 2011), but assumes that a substantial effort is made to reach citizens via multiple communication channels or media. Other ideas include obligatory classes in elementary and high-school or free/ subsidised night courses.

2.6 Development of over-arching nation-state cyber security strategies

The mid-1990s shift from seeing information infrastructures primarily as a tool for getting a competitive advantage (especially in the business world) towards recognising national dependency on information infrastructures as a nation-state interest ultimately brought the protection of (critical) information infrastructures (CII) on the agenda of security policy, as elaborated by Dunn (2005). With the cyber-attacks against Estonia in 2007 and successive major cyber-related incidents and the emerging threat posed by hacktivism (Denning, 2001; Ottis, 2010), cyber security as an "extension" of CII protection emerged, forcing nations to re-evaluate their national security frameworks. Estonia was among the first to develop a dedicated national cyber security strategy, implemented in 2008, in response to the attacks suffered, making changes to their legal, organisational and strategic framework (Czosseck *et al.,* 2011). Many more countries followed suit, including Austria and Great Britain in 2009, Canada and Japan in 2010 and France and Germany in 2011.

As such, this group of strategies reflects the process of developing and implementing a dedicated nation-state cyber security strategy or policy, and its subsequent reorganisation of nation-state responsibilities and authorities. This might include forming or further empowering specialised public bodies such as national CERTs, inter-ministry coordination centres like the German National Cyber Defence Centre, or centralisation of authority as in the Department of Homeland Security in USA.

2.7 Promotion and support of botnet hunting initiatives

A myriad of actors are currently investigating botnets, trying to monitor or infiltrate them, or to mitigate their effects on themselves or others. Botnets are an experimental subject of research and the basis for many business ideas.

Taking Microsoft's Digital Crime Unit, *a* "w*orldwide team of lawyers, investigators, technical analysts and other specialists whose mission is to make the Internet safer and more secure through strong enforcement, global partnerships, policy and technology solutions"* (Microsoft, 2011) serves as an example of a private sector initiative to coordinate actions against botnets. While public bodies are involved (especially in law enforcement) they do not play a leading role.

This group of strategies is understood as those active efforts of a nation-state to encourage, facilitate and perhaps even financially support similar initiatives dedicated to providing intelligence on or taking down botnets. This could include establishing devoted public bodies or points of contact to become part of such a cooperation, (financially) supporting intelligence efforts necessary to gather take-down information, or maybe even issuing a "bounty".

2.8 Software developers' obligations or incentives

Developing software was always prone to (exploitable) bugs and flaws in the concept. While extensive research has been carried out on how to develop secure software, the reality shows that there is still a long way to go. There are many reasons for this, but economically-motivated time-pressure and a lack of security-aware programmers might be two of the more dominant issues involved. While different international IT security evaluation and accreditation frameworks, like Common Criteria (CCRA 2012) exist, they are not obligatory for any software to be sold, and even less so for software made available for free/ open source.

This group of strategies includes efforts to increase the pressure on software developers to produce more secure (proven) code. There are a variety of instruments available, starting with the promotion of standards (such as Common Criteria), and successively the requirement for certified compliance with standards in public procurement. This might include the obligation to clearly indicate compliance to customers. Another method is the introduction of liability obligations to software developers, e.g. a mandate/ incentive for software developers to release security patches to all users, including those using illegal copies, or the responsibility for disclosure and fast patching (Anderson *et al.*, 2008).

2.9 Obligation of cyber insurances

Another idea circulated among scholars for some time, and received a greater jolt of governmental encouragement in 2002; Richard Clarke, the former cyber advisor to the Bush administration, met with insurance companies in the US to lobby for the coverage of cyber-based risks by them (Risen 2010). While initial estimations for the development of this market were over-optimistic, it was estimated to cost around 0.5 billion USD in 2010 (Risen, 2010); a market emerged providing different types of coverage ranging from breaches of data, regulatory civil action, cyber extortion, virus liability and many more as presented by Wood (2011).

This group of strategies reflects the state-driven encouragement of cyber insurances and the possible introduction of the obligation to be insured. This obligation could especially aim for key industries that are identified by a nation-state as critical.

2.10 National or international partnership programmes and information exchange

It is generally accepted that botnets have become a global issue, and that the instruments for fighting them are mainly in the hands of private sector. Nonetheless, with state-sponsored espionage and already evolving military cyber capabilities, the role of the nation-states increases.

Private-public partnership programmes have been identified as key by many nation-states, as well as the need for collaboration between key stakeholders. They might provide a platform for consultation, cooperation and information exchange, a starting point to initiate and later facilitate joined initiatives or reduce tension from competitive market participants so that they jointly introduce measures seen as unpleasant for their customer base.

This group of strategies represents the active promotion of, participation in and contribution to national and international partnership programmes. Examples of this can be seen in the Australian Internet Security Initiative, established in 2006 (ACMA, 2005) or the Dutch anti-botnet MoU between ISPs, signed in 2007 (Evron, 2009). In an international context, the European Public-Private Partnership for Resilience Programme (European Commission, 2010) and the London Action Plan (L.A.P., 2005) serve as examples.

3. Shortfalls, threats or missing capabilities

In this section, a selection of key problems of the botnet threat is presented. They build upon the findings of the sources introduced in the last section. They are either existing shortfalls, missing capabilities or alternatively they are threats or existing

problems. In both cases it would be "positive" if they are reduced by the strategies presented, and it would be "negative" if they are increased. They are the following:

A. (Improving) **detection, monitoring and tracking of botnets**
   As Plohmann *et al*. (2011) identified, it is still assumed that many botnets are not detected at all and the existing methods to survey identified botnets are not sufficiently developed. As such, an improvement in this category will lead to better situation awareness, ultimately enabling more precise actions to be taken against botnets. In addition, the difficult problem of (technical) attribution might be reduced.

B. (Reducing the) **existing botnet population**
   A strategy might have a direct influence on the existing population, leading to clean ups or at least the unavailability of these zombies for their bot master.

C. (Reducing the risk of) **new infections and migration to new victim platforms**
   Some of the strategies might have a preventative influence, raising the bar for bot masters who want to launch new or further spread existing botnets.

D. (Reducing profitability of the) **cyber-crime economy behind botnets**
   One major driving factor behind the current botnet issue is the fact that cyber-crime became highly profitable. A strategy might have a deterrent effect on people entering this "business", reduce the profit made or raise the arms race between good guys and bad guys to a level where the outcome is no longer worth the effort.

E. (Reducing/ deterring the) **botnet usage by APT or state sponsored espionage/CNO**
   Advanced Persistent Threat (APT) actors are increasingly reported as taking advantage of the existing botnet population, querying them for coincidentally infected zombies in or close to the target of their interest (GTISC & GTRI, 2011). Furthermore, there are an increasing number of cases where cyber-attacks are launched by actors who do not have a direct monetary interest but rather a state-driven political goal they wish to achieve. A strategy might have a deterrent effect on this type of botnet usage both now and in the future.

F. (Reducing/ deterring the) **botnet usage by hacktivism**
   Similar to state-sponsored activities, political goals are the driving factor behind hacktivism and have been introduced by e.g. Denning (2001). Similarly, strategies might have a deterrent effect on this group of people, who think and act slightly differently from "ordinary" criminals.

G. (Inhibiting the) **development and proliferation of botnet technology**
   Botnet developers and the stakeholders trying to fight them have already

entered a (mostly) technological arms race. Additionally, "botnets as a service" enables basically everyone willing to pay to get his hand on a botnet, dramatically increasing the access to them for everybody. The strategies presented in this article might have an influence on this proliferation.

4. DEMATEL analysis of the empirical data

Between 1972 and 1976, the Science and Human Affairs Program of the Battelle Memorial Institute of Geneva developed the *Decision-Making Trial and Evaluation Laboratory* (DEMATEL) method to research and solve clusters of complicated and intertwined problem groups called *problematiques*. Based on graph theory, problems can be planned and solved visually, dividing relevant factors into cause and effect groups to better understand causal relationships (Li & Tzeng, 2009).

It has be successfully applied in different domains such as knowledge management (Wu, 2008), policy impact on SMEs (Shyu, 2008), financial investment strategies (Lee, 2009) or strategic cyber security (Geers, 2011). The method is constantly extended and combined with other methods such as the maximum mean de-entropy algorithm (Li & Tzeng, 2009), fuzzy logic approaches (Lin & Wu, 2008; Tzeng *et al.*, 2009) or causal loops (Jafari *et al.*, 2008).

The four steps of the original DEMATEL method are: "(1) calculate the average matrix, (2) calculate the normalized initial direct-influence matrix, (3) derive the total relation matrix, and (4) set a threshold value and obtain the impact-relations map" and are explained in detail in (Li & Tzeng, 2009).

4.1 Input matrix

Based on the 10 strategy groups and seven effects presented in the earlier section, a questionnaire was developed and sent to experts in the field. Every strategy group and effect was pair-wise compared, and the interviewees were asked to assess the influence one has on the other on a scale from 0 to 3 with the latter being the greatest influence. (The DEMATEL method allows for any positive number as input, but scales from 0 – 3 are very common.)

In total 11 interviewees responded, covering seven countries and representing technical, strategic and legal viewpoints. Their individual answers were combined by calculating the average for every individual answer. This resulted in the initial input matrix presented as Table 1.

In the following tables, strategies are abbreviated by S1 – S10 and effects by E1 – E7, matching the corresponding sub-section numbers.

Table 5: Average input matrix T, based on questionnaire

	S1 R&D Programs	S2 Intern. law enforcement	S3 End User	S4 ISP obligations & incentives	S5 Awareness campaigns	S6 Cyber security strategies	S7 Botnet Hunting	S8 SW Developers' obligations	S9 Cyber Insurances	S10 Partnership programmes	E1 Detection of Botnets	E2 existing population	E3 new infections	E4 Cyber Crime Economy	E5 APT/state-sponsored usage	E6 Hacktivism botnet usage	E7 Technology proliferation	Total Influence
S1	0,0	0,4	0,9	0,8	1,3	1,5	2,0	0,8	0,5	2,0	2,3	1,4	1,0	0,5	0,4	0,5	0,7	17
S2	0,5	0,0	0,7	1,9	1,0	1,5	1,3	0,5	0,7	2,0	1,2	1,3	0,8	1,9	0,5	1,5	0,4	18
S3	0,5	0,7	0,0	1,9	2,5	1,3	1,0	0,7	0,9	1,6	1,3	2,1	1,3	1,2	0,2	0,6	0,5	18
S4	1,0	1,3	2,5	0,0	2,4	1,6	1,4	0,7	1,4	2,0	2,7	2,3	1,8	1,5	0,6	1,0	1,2	25
S5	0,8	0,7	2,2	0,8	0,0	1,3	1,2	0,5	0,6	0,6	0,6	1,4	1,5	0,9	0,1	0,4	0,3	14
S6	2,4	2,1	1,0	1,3	1,9	0,0	1,3	0,9	0,6	2,3	1,3	1,0	0,6	0,8	0,7	0,9	0,5	20
S7	2,1	1,6	0,9	1,3	1,1	1,1	0,0	0,3	0,2	1,9	2,9	2,0	1,0	1,4	0,8	0,9	1,2	21
S8	1,5	0,2	0,8	0,6	0,9	0,4	0,3	0,0	1,1	0,8	0,4	1,3	1,7	0,6	0,5	0,4	0,8	12
S9	0,9	0,4	1,4	1,3	1,2	0,8	0,6	1,2	0,0	0,6	1,0	0,7	0,7	0,4	0,2	0,4	0,2	12
S10	1,6	1,9	1,6	1,2	1,2	1,5	1,5	0,4	0,2	0,0	2,0	1,3	1,1	0,6	0,5	0,4	0,5	18
E1	1,6	1,5	1,1	1,1	0,8	0,7	2,1	0,2	0,3	2,1	0,0	1,8	1,1	1,2	0,6	0,9	0,8	18
E2	1,0	1,2	0,9	0,8	1,3	0,7	1,7	0,4	0,3	1,6	2,1	0,0	1,8	1,9	0,8	1,3	1,0	19
E3	1,2	0,3	0,7	0,6	1,0	0,8	0,9	0,4	0,2	1,0	1,6	1,9	0,0	1,4	0,6	0,6	1,1	14
E4	0,6	1,3	0,3	0,4	0,4	0,9	1,0	0,2	0,2	1,3	1,4	2,2	1,5	0,0	0,1	0,1	1,3	13
E5	0,9	1,0	0,1	0,3	0,3	1,8	0,7	0,1	0,2	0,9	0,7	0,5	0,7	0,4	0,0	0,6	0,4	10
E6	0,5	1,2	0,4	0,6	0,8	0,8	0,6	0,1	0,1	0,7	0,5	0,6	0,3	0,3	0,4	0,0	0,3	8
E7	0,9	0,5	0,6	0,7	0,4	0,7	1,2	0,7	0,1	1,1	1,6	1,8	2,0	1,0	0,6	0,5	0,0	14
Influenced by	**18**	**16**	**16**	**16**	**19**	**17**	**19**	**8**	**8**	**23**	**24**	**24**	**19**	**16**	**8**	**11**	**11**	

4.2 Direct influence analysis

The sum of the individual influence levels in each row is presented in the column "Direct influence". This expresses the total influence a strategy or botnet effect has, and allows for a first ranking of all strategies, as presented in Table 2.

ISP obligations & incentives being at the top is as expected, as are strategies targeting cyber insurance or software developers being at the very bottom. But it is surprising that broadly launched awareness campaigns also rank far below the average, with a score of 14.

Table 6: Total influence ranking of strategy groups

Strategy Group	Total Influence
S4 ISP obligations & incentives	25
S7 Botnet hunting	21
S6 Cyber security strategies	20
S2 Intern. law enforcement	18
S3 End-user	18
S10 Partnership programmes	18
S1 R&D Programmes	17
S5 Awareness campaigns	14
S8 SW Developers' obligations	12
S9 Cyber Insurances	12

In a similar manner, the empirical data allows for a ranking of the level of total influence the botnet threats receive, as presented in Table 3.

Table 7: Total influence level on botnet threat

Effect on botnet threat	Level influenced
E1 Detection of botnets	24
E2 Existing population	24
E3 New infections	19
E4 Cyber Crime Economy	16
E6 Hacktivism botnet usage	11
E7 Technology proliferation	11
E5 APT/state-sponsored usage	8

It becomes evident that addressing the more technical aspects of the botnet threat, meaning its detection and disinfections, is highly influential. On the other side, addressing the users of these botnets appears to be more limited.

4.3 Indirect influence

As Figure 1 illustrates, a strategy group can affect the botnet treat directly, but also indirectly. In the latter case it has a direct influence on another element, which in turn has a direct influence on the final element. This leads to the insight that a presumably strong direct influence of a given strategy group could be the result of multiple indirect influences. Over time, each of these indirect influences impacts every other element of the system, including itself.

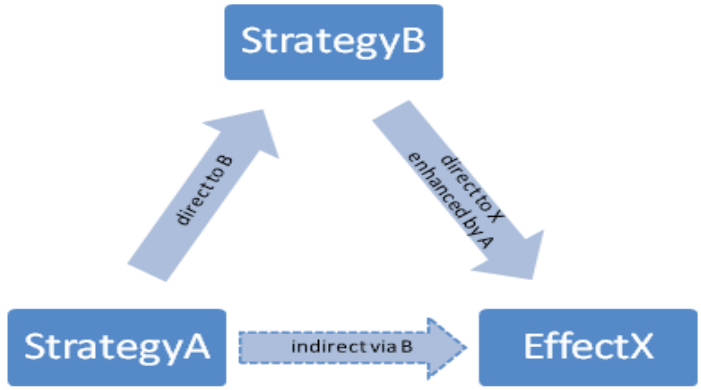

Figure 10: Indirect influence illustration

The DEMATEL method is capable of recognising this fact and can decompose direct and indirect influence by calculating the total relation matrix, $Q = M \times (I - M)^{-1}$, where M is the normalised matrix of T (see Table 1) and I is the identity matrix. Q is illustrated in Table 4.

Table 8: Total relation matrix, Q

	S1 R&D Programs	S2 Intern. law enforcement	S3 End User	S4 ISP obligations & incentives	S5 Awareness campaigns	S6 Cyber security strategies	S7 Botnet Hunting	S8 SW Developers' obligations	S9 Cyber Insurances	S10 Partnership programmes	E1 Detection of Botnets	E2 existing population	E3 new infections	E4 Cyber Crime Economy	E5 APT/state-sponsored usage	E6 Hacktivism botnet usage	E7 Technology proliferation	Direct Influence
S1	5.5	0,10	0,11	0,11	0,14	0,14	0,17	0,07	0,05	0,19	0,20	0,17	0,13	0,10	0,05	0,07	0,08	1,98
S2	0,11	0,09	0,11	0,15	0,13	0,14	0,15	0,06	0,06	0,19	0,17	0,17	0,12	0,15	0,06	0,11	0,07	2,02
S3	0,11	0,11	0,09	0,15	0,19	0,14	0,14	0,07	0,07	0,18	0,17	0,20	0,15	0,13	0,05	0,08	0,08	2,11
S4	0,16	0,17	0,21	0,11	0,22	0,18	0,19	0,08	0,10	0,23	0,26	0,25	0,20	0,17	0,08	0,12	0,12	2,85
S5	0,10	0,09	0,15	0,09	0,08	0,12	0,12	0,05	0,05	0,11	0,12	0,15	0,13	0,10	0,03	0,06	0,06	1,62
S6	0,19	0,17	0,13	0,14	0,17	0,10	0,16	0,08	0,06	0,21	0,18	0,17	0,12	0,12	0,07	0,10	0,08	2,23
S7	0,18	0,16	0,13	0,14	0,15	0,14	0,12	0,06	0,05	0,21	0,25	0,21	0,15	0,15	0,08	0,10	0,11	2,37
S8	0,12	0,06	0,08	0,07	0,10	0,07	0,08	0,03	0,07	0,10	0,10	0,13	0,13	0,08	0,04	0,05	0,07	1,37
S9	0,10	0,07	0,11	0,10	0,11	0,09	0,09	0,07	0,03	0,10	0,12	0,11	0,09	0,07	0,03	0,05	0,05	1,39
S10	0,15	0,16	0,14	0,13	0,14	0,14	0,16	0,05	0,05	0,12	0,20	0,17	0,13	0,11	0,06	0,07	0,08	2,06
E1	0,15	0,14	0,12	0,12	0,12	0,11	0,18	0,05	0,05	0,20	0,13	0,19	0,13	0,13	0,06	0,09	0,09	2,07
E2	0,13	0,13	0,12	0,11	0,14	0,11	0,16	0,05	0,05	0,18	0,20	0,12	0,16	0,16	0,07	0,11	0,10	2,10
E3	0,12	0,08	0,09	0,08	0,11	0,10	0,11	0,05	0,04	0,13	0,16	0,16	0,08	0,12	0,05	0,07	0,09	1,63
E4	0,09	0,11	0,07	0,07	0,08	0,10	0,11	0,04	0,03	0,14	0,15	0,17	0,13	0,07	0,04	0,05	0,09	1,55

E5	0,09	0,09	0,05	0,06	0,06	0,11	0,08	0,03	0,03	0,10	0,09	0,08	0,07	0,06	0,02	0,05	0,05	1,12
E6	0,06	0,09	0,05	0,06	0,07	0,07	0,07	0,02	0,02	0,08	0,08	0,08	0,05	0,05	0,03	0,03	0,04	0,97
E7	0,11	0,09	0,09	0,09	0,09	0,09	0,13	0,06	0,03	0,13	0,16	0,16	0,15	0,11	0,06	0,07	0,05	1,65
Indirect Influence	**2,05**	**1,92**	**1,85**	**1,78**	**2,10**	**1,94**	**2,22**	**0,89**	**0,84**	**2,59**	**2,73**	**2,67**	**2,11**	**1,88**	**0,89**	**1,28**	**1,31**	

4.4 Findings based on the adjusted influence index

With the direct and indirect influence present, one can easily calculate the difference between the direct influences and the indirect influences that each single strategy group received. This "adjusted influence" expresses the remaining influence that a single strategy has on the system. Table 5 illustrates this.

Table 9: Remaining influence on the system per strategy group

Strategy Group	**Direct Influence**	**Indirect Influence**	**Adjusted Influence**
S4 ISP obligations & incentives	2,85	1,78	1,07
S9 Cyber insurances	1,39	0,83	0,55
S8 SW developers' obligations	1,37	0,89	0,48
S6 Cyber security strategies	2,23	1,94	0,29
S3 End-user	2,11	1,85	0,25
S7 Botnet hunting	2,37	2,21	0,15
S2 Intern. law enforcement	2,02	1,91	0,11
S1 R&D programmes	1,98	2,05	-0,08
S5 Awareness campaigns	1,62	2,09	-0,48
S10 Partnership programmes	2,06	2,58	-0,53

The group "ISP obligations & incentives" again scores highest, confirming the initial observation and common assumption. What is more of a surprise is that the strategic groups *cyber insurances* and *software developers' obligations*, which were initially at the very end of the list, now rank second having about 50% less impact than the most influential group.

With about 25% of the impact of the most influential group, the groups *cyber security strategies* and *end-user obligations and good-behaviour* end in the third position, being ranking-wise the same, but in absolute terms are far lower in relation to the highest impact group.

The botnet hunting strategy group experiences another surprising rank change, now ending with only limited influence on the system, at around 10% of the best. Looking at the end of the table, R&D programmes, awareness campaigns and partnership programmes do score negatively. This means that their initial assumed impact on the system is mainly a result of indirect influences by other elements of the system.

Table 10: Remaining influence on the botnet threat per effect

Effect on Botnet Threat	Direct Influence	Indirect Influence	Adjusted Influence
E1 Detection of botnets	2,07	2,73	-0,66
E2 existing population	2,10	2,67	-0,58
E3 New infections	1,63	2,11	-0,49
E4 Cyber Crime Economy	1,55	1,88	-0,34
E6 Hacktivism botnet usage	0,97	1,28	-0,32
E5 APT/state-sponsored usage	1,12	0,89	0,23
E7 Technology proliferation	1,65	1,31	0,34

Looking at the effects on the botnet threat also reveals some interesting findings. Table 6 illustrates the adjusted influences, calculated in the same manner. Most of the possible effects on the botnet threat do have a negative influence value, meaning that they are developing into less of a threat, so are moving in "positive" directions. The only exceptions are the usage of botnets for state actors and the proliferation of botnet technology. This means that the strategy groups discussed in this paper act as a driver for these two and we will see a steady rise in them.

5. Conclusions

Botnets have become major cyber weapons, threatening nation-states' security and encouraging these nations to identify proper means to cope with them. This is a complex problem and, acknowledging that there are a multitude of factors to consider, this research has contributed in two ways. Firstly, it does so by establishing a framework of strategic options for nation-states to select from. Secondly, by applying the DEMATEL method on the data of the conducted survey, the system was analysed for the influence that each of the elements has. This allows for the ranking of the strategy groups, indicating the influence that each of them has on the botnet threat, as is presented in Table 5. The DEMATEL analysis revealed some interesting findings with regards to the influence order of the discussed strategic option.

The common opinion about the crucial and influential role that ISPs play in the fight against botnets has been confirmed. The greatest surprise is that *cyber*

insurances and *software developers' obligations* scored so highly in the influence ranking, as they are commonly regarded as less feasible. The limitation of the conducted research is that it did not consider the difficulties one might face by implementing a certain strategy. On the other hand, this can turn into an advantage as implementation concerns are less likely to influence the findings, encouraging future research.

Also remarkable is the fact that the influence of the analysed groups drops in steps of roughly factor 2. The presented ranking by influence allows for easy selection of preferable strategies and can serve as an input for decision makers. With regards to the effect on the botnet threat, it is remarkable to see that state-driven usage of botnets and technology proliferation is not influenced in a mitigating way at all. While it might be assumed for the latter, it is surprising for the former.

References

ACMA, 2005. *ACMA - Australian Internet Security Initiative.* ACMA. Available at: http://www.acma.gov.au/WEB/STANDARD/pc=PC_310317 [Accessed January 16, 2012].

Anderson, R. et al., 2008. *Security Economics and the Internal Market*, ENISA.

Asghari, H., 2010. *Botnet Mitigation and the Role of ISPs*. Delft University of Technology.

BBC, 2011. *BBC News - French downloaders face government grilling*. Available at: http://www.bbc.co.uk/news/technology-14294517 [Accessed January 11, 2012].

CCC, 2011. *Cyber Clean Center*. Available at: https://www.ccc.go.jp/en_index.html [Accessed January 11, 2012].

CCRA, 2012. *Common Criteria : The Common Criteria Portal*. Available at: http://www.commoncriteriaportal.org/ [Accessed January 13, 2012].

Cabinet Office UK & Detica Ltd., 2011. *The Cost of Cyber Crime*.

Council of Europe, 2001. *Convention on Cybercrime.* Available at: http://conventions.coe.int/treaty/en/treaties/html/185.htm.

Czosseck, C. & Podins, K., 2011. An Usage-Centric Botnet Taxonomy. In *Proceedings of the 10th European Conference on Information Warfare and Security*. Tallinn: ECIW, pp. 65-72.

Czosseck, C., Ottis, R. & Talihärm, A.-M., 2011. Estonia after the 2007 Cyber Attacks. *International Journal of Cyber Warfare and Terrorism*, 1(1), pp.24-34.

Denning, D.E., 2001. Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy. In *Networks and netwars: The future of terror, crime, and militancy*, pp.239–288.

Dunn, M., 2005. A comparative analysis of cybersecurity initiatives worldwide. In *WSIS Thematic meeting on Cybersecurity, Geneva*.

ECO, 2011. *Anti-Botnet-Beratungszentrum.* Available at: https://www.botfrei.de/en/index.html [Accessed January 11, 2012].

Eeten, M.V. et al., 2010. The role of internet service providers in botnet mitigation: an empirical analysis based on spam data. *OECD Science, Technology and Industry Working Papers*, 2010/05.

European Comission, 2007. *COM (2007) 697*. Available at: http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=196418 [Accessed January 11, 2012].

European Commission, 2010. *European Public-Private Partnership for resilience –EP3R*. Available at: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/ep3r/index_en.htm [Accessed January 16, 2012].

Evron, G., 2009. *Dutch ISPs Sign Anti-Botnet Treaty - Dark Reading*. darkreading. Available at: http://www.darkreading.com/blog/227700601/dutch-isps-sign-anti-botnet-treaty.html [Accessed January 16, 2012].

GTISC & GTRI, 2011. *Emerging Cyber Threats Report 2012*,

Geers, K., 2011. *Strategic Cyber Security : Evaluating Nation-State Cyber Attack Mitigation Strategies with DEMATEL* Faculty of Information Technology. TUT.

Jafari, M., Hesam, R. & Bourouni, A., 2008. An Interpretive Approach to Drawing Causal Loop Diagrams. In *Proceedings of the 26th International Conference of the System Dynamics Society: 20-24 July 2008; Athens Greece*.

L.A.P., 2005. *London Action Plan*. Available at: http://www.londonactionplan.com/ [Accessed January 16, 2012].

Lee, W.S.A.Y.H.C.-C.C., 2009. Financial Investment Strategy by DEMATEL and Analytic Network Process. *Network*.

Li, C.-W. & Tzeng, G.-H., 2009. Identification of a threshold value for the DEMATEL method using the maximum mean de-entropy algorithm to find critical services provided by a semiconductor intellectual property mall. *Expert Systems with Applications*, 36(6), pp.9891-9898.

Lin, C.J. & Wu, W.W., 2008. A causal analytical method for group decision-making under fuzzy environment. *Expert Systems with Applications*, 34(1), pp.205–213.

Microsoft, 2011. *Microsoft Digital Crimes Unit*. Available at: https://www.microsoft.com/presspass/presskits/DCU/ [Accessed January 13, 2012].

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

Ottis, R., 2010. From Pitchforks to Laptops Volunteers in Cyber Conflicts. In C. Czosseck & K. Podins, eds. *Conference on Cyber Conflict Proceedings*. Tallinn: CCD COE Publications, pp. 97 - 108.

Plohmann, D., Gerhards-Padilla, E. & Leder, F., 2011. Botnets: Detection, Measurement, Disinfection & Defence. *Information Security*, p.153.

Risen, T., 2010. Can Insurers Protect The U.S. From Cyber-Attack? - Tom Risen - NationalJournal.com. *National Journal*. Available at: http://www.nationaljournal.com/njonline/no_20100208_9513.php [Accessed January 13, 2012].

Shyu, J.Z., 2008. Causal relationship analysis based on DEMATEL technique for innovative policies in SMEs. *PICMET 08 2008 Portland International Conference on Management of Engineering Technology*, (c), pp.373-379.

Tzeng, G.-H. et al., 2009. Fuzzy decision maps: a generalization of the DEMATEL methods. *Soft Computing*, 14(11), pp.1141-1150.

Wood, L., 2011. Got cyber insurance? *Network World*. Available at: http://www.networkworld.com/news/2011/102411-cyber-insurance-252145.html [Accessed January 13, 2012].

Wu, W., 2008. Choosing knowledge management strategies by using a combined ANP and DEMATEL approach. *Expert Systems with Applications*, 35(3), pp.828-835.

CONCLUSIONS

The threat posed by malicious cyber activities with botnets being one major tool is both topical and challenging. The research presented here aimed to support policy makers and national security advisers in their on-going efforts to mitigate the threat posed by botnets towards national cyber security.

Cyber security is a complex and multi-disciplinary challenge, combining the need to draw from information technology, strategic management and cyber conflict research.

Summary of Key Findings

Considering the wider context, which needs to be considered when making informed decisions, the research presents the following findings:

1. Cyber weapons include many of the characteristics and principles of conventional weapons, but in addition include new features and attributes to such an extent that models based on conventional weapons are no longer suitable for cyber weapons.
2. The understanding of vulnerabilities in IT systems becomes a strategic good in cyber conflict. The capability to discover and exploit them directly translates into offensive and defensive cyber space capabilities.
    - Cyber weapons can be destroyed by disclosing the vulnerability used as the basis of their effect. This provides a method for disarming cyber weapons in cyberspace.
    - Assuming rational behaviour, the destruction of ones cyber weapons through the disclosure of the underlying vulnerability does not affect this party's cyber defence capabilities.
3. The original role of botnets as the primary tool for cyber criminals to illegally access financial gains has shifted towards becoming a tool for different actors in cyber space with different aims and motivations. Therefore, organizations in the private and public sectors need to consider the likelihood of being the target of botnet mounted attacks beyond the scope of cyber crime.

If we consider an organization-level response to an immanent or on-going botnet mounted cyber attack, especially a DDoS attack:

4. It was suggested that with the technology available, a sustainable organizational-level botnet takedown of a concrete botnet is difficult or impossible mainly due to the legal restrictions and the need for time consuming analysis and/or global coordination efforts.

- While botnet takedowns are possible, they required proper (legal) authorization, which is mostly not available.
- The need for international cooperation and coordination currently slows takedown attempts to the point that a swift response is not possible.
- The developers of botnets have the upper hand and the IT security industry faces noticeable challenges in getting back on top of the issue.
- Botnet technology is in most cases easy and cheap to acquire and easy to set up resulting in low barriers to botnet use.

If we consider the strategy options for a State seeking to mitigate the effect of botnets:

5. A comprehensive framework of 10 State-level strategies to mitigate the botnet threat has been developed and presented.
6. Their efficiency has been evaluated using the DEMATEL method and empirical data leading to prioritized recommendations as follows:
   1. Priority: *ISP Obligations & Incentives* were confirmed as the best strategy to follow, having the highest impact.
   2. Priority: The effect of *Cyber Insurances*, *Software Developers' Obligations* and *Botnet Hunting Initiatives* is underrated in public opinion and it is recommended that these be considered more actively.
   3. Priority: Developing *national Cyber Security Strategies*, *End-user Obligations and Good-behaviour Incentives* and *International Law Enforcement Agreements* are still valid options.
   4. Priority: **Desist in** investing in *Partnership Programmes*, *Awareness Campaigns* or *R&D Programmes* with the latter being a borderline call.

7. The model developed here further predicts that the proliferation of botnet technology and the likelihood of botnet use by state actors will increase.

Limitations and Critique

The research presented here focuses on and therefore limited its scope to the threat posed by botnets.

The strategic options were only evaluated on the basis of their expected influence on the botnet threat. The costs or barriers to their implementation were not taken into account, and it is acknowledged that policy makers have to also consider political considerations in their decisions.

In addition, the evaluation was conducted on a highly abstract level clustering similar State-level strategy options into larger groups and evaluating them *en bloc*, which seemed appropriate at this stage of the research.

While the DEMATEL method has been successfully applied by developing an influence model and successively evaluating State-level botnet mitigation Strategy options, this approach is limited in two respects:

- Firstly, as the developed influence model consists of 17 elements in total, this resulted in nearly 300 pair-wise comparisons to be made by each interviewed expert contributing to the collection of the empirical data. While each single question was quickly answered, the sheer number of questions dramatically reduced the number of responses in the interviews.
- As a result, and secondly, only 11 experts responded to the invitation to the interview. Nevertheless, all of them were recognized in their field and represented a wide distribution of expertise from industry, government and academia, as well as having backgrounds in technology, management and law.

Ultimately, we can have confidence in the findings because, due to the number of experts involved, the likelihood of errors was reduced by a factor of approximately 3.5, giving the findings sufficient significance.

Suggestions for Future Research

Building on this research and in order to overcome the current limitations, future research could continue as follows:

- Redesign the evaluation method by combining DEMATEL with other methods, such as AHP, to reduce the complexity of the questionnaire for collecting the empirical data, hopefully resulting in a higher response rate.
- The findings of this research were constructed using a high level of abstraction in the form of evaluating strategy *groups*. In the next step, those groups identified as promising could be decomposed into their single strategies and the analysis repeated at a higher level of detail.
- The research findings should be further enhanced by applying quantitative methods to confirm that a particular strategy indeed has a noticeable effect[32]. Future research could also develop a model to measure the level of cyber security in a country. Ideally, this could be done via quantitative means.
- To explore further ways to measure the performance of the implementation of a cyber security strategy and/or single action.
- To extend the botnet focused threat model by covering all cyber threats, including especially targeted and hacktivism-motivated malicious cyber activities.

[32] At the time of this research many of the identified strategy groups were only implemented in a few, sometimes even only one nation. Others were in the process of adopting them. As such their effect should only appear after some years.

- To develop means for discussing and evaluating costs or barriers related to the implementation of the strategies discussed.
- The research conducted here compared cyber weapons with conventional weapons only. The findings suggest extending this comparison to include all known weapons and methods of operation to discover further similarities between them and cyber weapons.
- The vulnerability-based model of cyber conflicts developed here seems to have the potential to be further developed to reduce its current limitations and assumptions. The next steps could be to introduce the notion of time or the severity of the exploit used.

REFERENCES

ACMA. 2005. ACMA - Australian Internet Security Initiative. *ACMA*. http://www.acma.gov.au/WEB/STANDARD/pc=PC_310317 (Accessed: 16. January 2012).

Adkins, Bonnie N. 2001. The Spectrum of Cyber Conflict from Hacking to Information Warfare: What is Law Enforcement's Role? US Air Command and Staff College.

Anderson, Ross, Rainer Boehme, Richard Clayton and Tyler Moore. 2008. Security Economics and the Internal Market. Heraklion: European Network and Information Security Agency.

Andrews, K.R. 1987. *The Concept of Corporate Strategy*. Ed. Richard D. Irwin. 3rd ed. New York: R. D. Irwin.

Applegate, Scott D. 2012. The Principle of Maneuver in Cyber Operations. In: *2012 4th International Conference on Cyber Conflicts*, ed. Christian Czosseck, Katharina Ziolkowski, and Rain Ottis, 183–195. Tallinn: CCD COE Publications.

Arimatsu, Louise. 2012. A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations. In: *2012 4th International Conference on Cyber Conflicts*, ed. Christian Czosseck, Katharina Ziolkowski, and Rain Ottis, 91–109. Tallinn: CCD COE Publications.

Berg, T. 2007. The Changing Face of Cybercrime New Internet Threats Create Challenges to Law Enforcement. *Michigan Bar Journal*, 1.

Billo, Charles and Welton Chang. 2004. Cyber Warfare an Analysis of the Means and Motivations of Selected Nation States. Hanover: Institute for Security Technology Studies at Dartmouth College.

Bozeman, Barry and Jeffrey D. Straussman. 1990. *Public management strategies: Guidelines for Managerial Effectiveness*. 1st ed. Jossey-Bass (San Francisco).

Bracker, J. 1980. The Historical Development of the Strategic Management Concept. *Academy of Management Review* 5, 2: 219–224.

Brenner, SW. 2002. Organized Cybercrime - How Cyberspace May Affect the Structure of Criminal Relationships. *NCJL & Tech.* 4, 1: 1–50.

Bryson, John M. 1988. Strategic Planning for Public and Nonprofit Organizations. *Long Range Planning* 21, 1 (February): 73–81. doi:10.1016/0024-6301(88)90061-1.

---. 2004. *Strategic Planning for Public and Nonprofit Organizations: A Guide to Strengthening and Sustaining Organizational Achievement*. 3rd ed. San Francisco: Jossey-Bass.

CCC. 2011. Cyber Clean Center. https://www.ccc.go.jp/en_index.html (Accessed: 11. January 2012).

Cavelty, Myriam Dunn. 2008. Cyber-Terror - Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. *Journal of Information Technology & Politics* 4, 1 (April): 19–36. doi:10.1300/J516v04n01_03.

---. 2012. The Militarisation of Cyberspace: Why Less May Be Better. In: *2012 4th International Conference on Cyber Conflicts*, ed. Christian Czosseck, Katharina Ziolkowski, and Rain Ottis, 141–153. Tallinn: CCD COE Publications.

Chandler, A.D. 2003. *Strategy and Structure*. reprinted. Washington, D. C.: Beard Books.

Charvat, J.P. 2009. Cyber Terrorism: A New Dimension in Battlespace. In: *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers. Amsterdam: IOS Press.

Chou, Tsung-yu and Yen-ting Chen. 2012. Applying DEMATEL to Improve Library Service Quality 2012: 1–18.

Chu, HC, DJ Deng and HC Chao. 2009. Next Generation of Terrorism: Ubiquitous Cyber Terrorism with the Accumulation of all Intangible Fears. *Journal of Universal Computer* 15, 12: 2391–2404.

Command Five Pty Ltd. 2011. Advanced Persistent Threats : A Decade in Review. http://www.commandfive.com/research.html (Accessed: 1. January 2012).

Conficker Working Group. 2009. Infection Maps. http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionDistribution (Accessed: 1. July 2012).

Cornish, Paul, David Livingstone, Dave Clemente and Claire Yorke. 2010. *On Cyber Warfare*. London: Chatham House.

Correll, Sean-Paul. 2010. 'Tis the Season of DDoS – WikiLeaks Edition | PandaLabs Blog. http://pandalabs.pandasecurity.com/tis-the-season-of-ddos-wikileaks-editio/ (Accessed: 9. February 2011).

Council of Europe. 2001. Convention on Cybercrime. http://conventions.coe.int/treaty/en/treaties/html/185.htm (Accessed: 1. January 2012).

---. 2005. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. *Official Journal L 69*: 67–71.

---. 2012. The Council of Europe and Cybercrime - FactSheet. https://wcd.coe.int//ViewDoc.jsp?Ref=FS+11&Language=lanEnglish&Ver=original&BackColorInternet=F5CA75&BackColorIntranet=F5CA75&BackColorLogged=A9BACE (Accessed: 1. January 2012).

Crosby, Benjamin L. 1991. Strategic Planning and Strategic Management: What Are They and How Are They Different? A publication of USAID's Implementing Policy Change Project.

Czosseck, Christian, Rain Ottis and A.M. Talihärm. 2011. Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security. *International Journal of Cyber Warfare and Terrorism (IJCWT)* 1, 1: 24–34.

Dagon, David, Guofei Gu, Christopher P. Lee and Wenke Lee. 2007. A Taxonomy of Botnet Structures. *Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007)* (December): 325–339. doi:10.1109/ACSAC.2007.44.

Dandurand, Luc. 2011. Rationale and Blueprint for a Cyber Red Team Within NATO An Essential Component of the Alliance' s Cyber Forces. In: *2011 3rd International Conference on Cyber Conflicts*, ed. Christian Czosseck, Enn Tyugu, and Thomas C. Wingfield. Tallinn: CCD COE Publications.

Denning, D. E. 2001a. Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy. *Networks and netwars: The future of terror, crime, and militancy*: 239–288.

---. 2001b. Obstacles and Options for Cyber Arms Control. In: *Proceedings of Arms Control in Cyberspace*, 1–13. Berlin: Heinrich Böll Foundation.

Drechsler, Wolfgang. 2005. The Rise and Demise of the New Public Management. *Post-Autistic Economics Review*, 33: 17–28.

Dunn, M. 2005. A comparative analysis of cybersecurity initiatives worldwide. In: *WSIS Thematic meeting on Cybersecurity, Geneva*.

ECO. 2011. Anti-Botnet-Beratungszentrum. https://www.botfrei.de/en/index.html (Accessed: 11. January 2012).

Eeten, Michel Van, J Bauer, Hadi Asghari and Shirin Tabatabaie. 2010. The role of internet service providers in botnet mitigation: an empirical analysis based on spam data. *OECD Science, Technology and Industry Working Papers* 2010/05. doi:10.1787/5km4k7m9n3vj-en.

European Commission. 2007. COM (2007) 697 - Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directives 2002/21/EC. http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=196418 (Accessed: 11. January 2012).

---. 2010. European Public-Private Partnership for resilience – EP3R. http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/ep3r/index_en.htm (Accessed: 16. January 2012).

---. 2011a. Proposal on a European Strategy for Internet Security. http://ec.europa.eu/governance/impact/planned_ia/docs/2012_infso_003_european_internet_security_strategy_en.pdf (Accessed: 13. September 2012).

---. 2011b. Critical Information Infrastructure Protection. http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm (Accessed: 16. January 2012).

Evron, Gadi. 2009. Dutch ISPs Sign Anti-Botnet Treaty - Dark Reading. *darkreading*. http://www.darkreading.com/blog/227700601/dutch-isps-sign-anti-botnet-treaty.html (Accessed: 16. January 2012).

Farivar, Cyrus. 2009. A Brief Examination of Media Coverage of Cyberattacks (2007 - Present). In: *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers, 182 – 188. Amsterdam: IOS Press. doi:10.3233/978-1-60750-060-5-182.

Fisher, Dennis. 2010. Waledac Botnet Now Completely Crippled, Experts Say | threatpost. *threatpost*. http://threatpost.com/en_us/blogs/waledac-botnet-now-completely-crippled-experts-say-031610 (Accessed: 16. January 2012).

---. 2011. Microsoft, FireEye Take Down Notorious Rustock Botnet | threatpost. *threatpost*. http://threatpost.com/en_us/blogs/microsoft-fireeye-take-down-notorious-rustock-botnet-031811 (Accessed: 16. January 2012).

Fritz, J. 2008. How China will use cyber warfare to leapfrog in military competitiveness. *Culture Mandala: The Bulletin of the Centre for* 8, 1.

GTISC and GTRI. 2011. Emerging Cyber Threats Report 2012. *Georgia Tech Cyber Security Summit 2011*. http://www.gtisc.gatech.edu/doc/emerging_cyber_threats_report2012.pdf (Accessed: 13. September 2012).

Gandhi, Robin, Anup Sharma, William Mahoney, William Sousan, Qiuming Zhu and Phillip Laplante. 2011. Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political. *IEEE Technology and Society Magazine* 30, 1 (January): 28–38. doi:10.1109/MTS.2011.940293.

Geers, Kenneth. 2011. *Strategic Cyber Security: Evaluating Nation-State Cyber Attack Mitigation Strategies with DEMATEL*. Doctoral Thesis: Faculty of Information Technology, Tallinn University of Technology.

Giles, Keir. 2011. "Information Troops" – a Russian Cyber Command? In: *2011 3rd International Conference on Cyber Conflicts*, ed. Christian Czosseck, Enn Tyugu, and Thomas C. Wingfield. Tallinn: CCD COE Publications.

---. 2012. Russia' s Public Stance on Cyberspace Issues. In: *2012 4th International Conference on Cyber Conflicts*, ed. Christian Czosseck, Katharina Ziolkowski, and Rain Ottis, 63–75. Tallinn: CCD COE Publications.

Gordon, Jason. 2008. Cyber Weaponization: Analysis of Internet Arms Development. *Computer Security Conference, Myrtle Beach, SC*.

Hare, Forrest. 2010a. The Interdependent Nature of National Cyber Security: Motivating Private Action for a Public Good. Doctoral Thesis: School of Public Policy, George Mason University.

---. 2010b. The Cyber Threat to National Security Why Can't We Agree. In: *Conference on Cyber Conflict*, ed. Christian Czosseck and Karlis Podins, 211 – 226. Tallinn: CCD COE Publications.

---. 2012. The Significance of Attribution to Cyberspace Coercion : A Political Perspective. In: *2012 4th International Conference on Cyber Conflicts*, ed. Christian Czosseck, Katharina Ziolkowski, and Rain Ottis, 125–139. Tallinn: CCD COE Publications.

Health Sector Reform Initiative. 2000. Policy Toolkit for Strengthening Health Sector Reform. Health Sector Reform Initiative.

Herley, Cormac and Dinei Florêncio. 2010. Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy. In: *Economics of Information Security and Privacy*, ed. Tyler Moore, David Pym, and Christos Ioannidis, 33–53. doi:10.1007/978-1-4419-6967-5_3.

Hofer, Charles W. 1978. *Strategy formulation: Analytical concepts*. St. Paul: West Pub. Co.

Hughes, Rex. 2009. Towards a Global Regime for Cyber Warfare. In: *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers. Amsterdam: IOS Press.

Hyacinthe, Berg. 2012. Law of Armed Conflicts Applied to i-Warfare and Information Operations: How and Under What Legal Framework Should Surgical NATO and U . S . Military Drone Strikes be Conducted ? In: *11th European Conference on Information Warfare and Security*, ed. Eric Filiol and Robert Erra, 313–319. Laval.

Iland, Daniel. 2010. The Emergence of Highly Customizable Malware. Rochester Institute of Technology. http://www.dannyiland.com/TheEmergenceofHighlyCustomizableMalware.pdf (Accessed: 26. August 2012).

Janczewski, Lech. 2008. *Cyber Warfare and Cyber Terrorism*. Ed. Lech Janczewski and Andrew M. Colarik. London: IGI Global.

Jellenc, Eli. 2012. Explaining Politico-Strategic Cyber Security : The Feasibility of Applying Arms Race Theory. In: *11th European Conference on Information Warfare and Security*, ed. Eric Filiol and Robert Erra, 151–162. Laval.

Kanwal, Gurmeet. 2009. China' s Emerging Cyber War Doctrine. *Journal of Defence Studies* 3, 3: 14–22.

Killourhy, K.S., R.a. Maxion and K.M.C. Tan. 2004. *A defense-centric taxonomy based on attack manifestations*. *International Conference on Dependable Systems and Networks, 2004*. IEEE. doi:10.1109/DSN.2004.1311881.

Kirillov, Ivan, D Beck, Penny Chase and Robert Martin. *Malware Attribute Enumeration and Characterization*. *al3x.org*.

Klein, Gabriel, Felix Leder and Christian Czosseck. 2011. On the Arms Race Around Botnets - Setting Up and Taking Down Botnets. In: *2011 3rd International Conference on Cyber Conflicts*, ed. Christian Czosseck, Enn Tyugu, and Thomas C. Wingfield. Tallinn: CCD COE Publications.

Klijn, E.H. and J.F.M. Koppenjan. 2000. Public management and policy networks: Foundations of a network approach to governance. *Public Management an International Journal of Research and Theory* 2, 2: 135–158.

Kola, Mahathi Kiran. 2008. Botnets: Overview and Case Study. Master Thesis: Department of Mathematics and Computer Information Science, Mercy College.

Krekel, Bryan, George Bakos and Christopher Barnett. 2009. Capability of the People' s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation. Northrop Grumman Corporation.

Landler, Mark and John Markoff. 2007. In Estonia, what may be the first war in cyberspace. *The New York Times*, 28. May.

Leder, Felix, Tillmann Werner and Peter Martini. 2009. Proactive Botnet Countermeasures An Offensive Approach. In: *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers. Amsterdam: IOS Press.

Lee, Wen-Shiung, Alex YiHou Huang, Yong-Yang Chang and Chiao-Ming Cheng. 2011. Analysis of decision making factors for equity investment by DEMATEL and Analytic Network Process. *Expert Systems with Applications* 38, 7 (July): 8375–8383. doi:10.1016/j.eswa.2011.01.027.

Lelli, Andrea. 2009. Trojan.Whitewell: What's your (bot) Facebook Status Today? | Symantec Connect Community. *Symantec*. http://www.symantec.com/connect/blogs/trojanwhitewell-what-s-your-bot-facebook-status-today (Accessed: 9. July 2012).

Lewis, JA. 2010. The Cyber War Has Not Begun. *Center for Strategic and International Studies*, March: 1–4.

Lewis, James A. and Katrina Timlin. 2011. *Cybersecurity and Cyberwarfare*. Washington: Center for Strategic and International Studies.

Li, Chung-Wei and Gwo-Hshiung Tzeng. 2009. Identification of a threshold value for the DEMATEL method using the maximum mean de-entropy algorithm to find critical services provided by a semiconductor intellectual property mall. *Expert Systems with Applications* 36, 6 (August): 9891–9898. doi:10.1016/j.eswa.2009.01.073.

Libicki, Martin C. 2009. Sub Rosa Cyber War. In: *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers. Amsterdam: IOS Press.

Liles, Samuel. 2010. Cyber Warfare: As a form of low-intensity conflict and insurgency. In: *Conference on Cyber Conflict Proceedings*, ed. Christian Czosseck and Karlis Podins, 47 – 57. Tallinn: CCD COE Publications.

Lin, Chia-Li and Gwo-Hshiung Tzeng. 2009. A value-created system of science (technology) park by using DEMATEL. *Expert Systems with Applications* 36, 6 (August): 9683–9697. doi:10.1016/j.eswa.2008.11.040.

Lorents, Peeter and Rain Ottis. 2010. Knowledge based Framework for Cyber Weapons and Conflict. In: *Conference on Cyber Conflict*, ed. Christian Czosseck and Karlis Podins, 129 – 142. Tallinn: CCD COE Publications.

Ludlow, Peter. 2010. WikiLeaks and Hacktivist Culture. *The Nation*, October 4: 25–27.

Mahoney, J. 2006. A Tale of Two Cultures: Contrasting Quantitative and Qualitative Research. *Political Analysis* 14, 3 (14. June): 227–249. doi:10.1093/pan/mpj017.

Mansfield-Devine, Steve. 2011. Hacktivism: assessing the damage - what's the real significance of Anonymous and LulzSec? *WebVivant*. http://www.webvivant.com/feature-hacktivism.html (Accessed: 9. July 2012).

Marquand, Robert and Ben Arnoldy. 2007. China emerges as leader in cyberwarfare. *The Christian Science Monitor*.

McGee, Joshua. 2011. NATO and Cyber Defence. http://www.nato-pa.int/default.asp?SHORTCUT=1782 (Accessed: 9. July 2012).

McLaughlin, Victoria. 2012. Anonymous: What do we have to fear from hacktivism, the lulz, and the hive mind? Bachelor Thesis: University of Virginia.

Microsoft. 2011. Microsoft Digital Crimes Unit. https://www.microsoft.com/presspass/presskits/DCU/ (Accessed: 13. January 2012).

Mintzberg, H, B Ahlstrand and Joseph Lampel. 1998. *Strategy Safari: A Guided Tour Through the Wilds of Strategic Management*. *New York*. 1st editio. New York: The Free Press.

NATO. 2008. NATO Summit Bucharest 2008 Declaration. http://www.summitbucharest.ro/en/doc_201.html (Accessed: 27. August 2012).

---. 2010. Strategic Concept for the Defence and Security of the Members of the NATO. http://www.nato.int/cps/en/natolive/official_texts_68580.htm (Accessed: 30. December 2010).

---. 2011. Defending the networks - The NATO Policy on Cyber Defence. http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf (Accessed: 9. July 2012).

NATO Parlamentary Assembly. 2009. NATO and Cyber Defense: A Brief Overview and Recent Events | Center for Strategic and International Studies. http://csis.org/blog/nato-and-cyber-defense-brief-overview-and-recent-events (Accessed: 9. July 2012).

Nazario, Jose. 2009a. Politically Motivated Denial of Service Attacks. In: *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers, 163–181. Amsterdam: IOS Press.

---. 2009b. Twitter-based Botnet Command Channel | DDoS and Security Reports | Arbor Networks Security Blog. *Arbor Sert*. http://ddos.arbornetworks.com/2009/08/twitter-based-botnet-command-channel/ (Accessed: 9. July 2012).

Nicholson, Andrew, Tim Watson, Peter Norris, Alistair Duffy and Roy Isbell. 2012. A Taxonomy of Technical Attribution Techniques for Cyber Attacks. In: *11th European Conference on Information Warfare and Security*, ed. Eric Filiol and Robert Erra, 188–197. Laval.

Nickols, Fred. 2011. Strategy, Strategic Planning, Strategic Thinking, Strategic Management. *Management Services*. Distance Consulting LLC.

Nissenbaum, H. 2005. Where Computer Security Meets National Security. *Ethics and Information Technology* 7, 2: 61–73.

OECD. 2008. Malicious Software (Malware): A Security Threat to the Internet Economy. OECD.

Ottis, Rain. 2008. Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. In: *Proceedings of the 7th European Conference on Information Warfare*, 163. Academic Conferences Limited.

---. 2010. From Pitchforks to Laptops Volunteers in Cyber Conflicts. In: *Conference on Cyber Conflict*, ed. Christian Czosseck and Karlis Podins, 97 – 108. Tallinn: CCD COE Publications.

---. 2011. A Systematic Approach to Offensive Volunteer Cyber Militia. Tallinn University of Technology.

Pavlyuchenko, Fyodor. 2009. Belarus in the Context of European Cyber Security. In: *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers. Amsterdam: IOS Press.

Perez, Sarah. 2009. Researchers Discover Botnet Commanded by Google Groups. *RedWriteWeb*. http://www.readwriteweb.com/archives/botnet_commanded_by_google_groups.php (Accessed: 9. July 2012).

Perry, WG. 2007. Information Warfare: An Emerging and Preferred Tool of the People's Republic of China. *Occasional Papers Series*, 28.

Plohmann, Daniel, Elmar Gerhards-Padilla and Felix Leder. 2011. *Botnets: Detection, Measurement, Disinfection & Defence*. *Information Security*. ENISA.

Porter, M.E. 1996. What is Strategy? *Harvard Business Review* 74, 6: 61 – 80.

Pras, Aiko, Anna Sperotto, G Moura and Idilio Drago. 2010. Attacks by "Anonymous" WikiLeaks Proponents not Anonymous. Enschede: University of Twente.

Remenyi, D and A Money. 2006. *Research supervision for supervisors and their students*. 2nd ed. Curtis Farm: Academic Conferences Limited.

Reuters. 2012. Cyber espionage on the rise, energy assets most vulnerable - The Economic Times. *The Economic Times*, 31. May.

Russell, Alec. 2004. CIA plot led to huge blast in Siberian gas pipeline. *The Telegraph*, 28. February.

Rutkowska, Joanna. 2006. Introducing Stealth Malware Taxonomy. COSEINC Advanced Malware Labs. http://66.14.166.45/whitepapers/compforensics/malware/rk/Introducing Stealth Malware Taxonomy.pdf (Accessed: 1. January 2012).

Safire, William. 2004. The Farewell Dossier. *The New York Times*, February.

Schmitt, Michael N. 1999. Computer network attack and the use of force in international law: thoughts on a normative framework. *Columbia Journal of Transnational Law* 37: 885–937.

---. 2002. Wired warfare: Computer network attack and jus in bello. *International Review Red Cross* 84, June: 365–400.

---. 2012. " Attack " as a Term of Art in International Law: The Cyber Operations Context. In: *2012 4th International Conference on Cyber Conflicts*, ed. Christian Czosseck, Katharina Ziolkowski, and Rain Ottis, 283–293. Tallinn: CCD COE Publications.

Scribner, S. 2000. Introduction to Strategic Management. In: *Policy Toolkit for Strengthening Health Sector Reform*, 164 – 170. Health Sector Reform Initiative.

Sharma, Amit. 2009. Cyber Wars: A Paradigm Shift from Means to Ends. In: *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers, 34:62–73. Amsterdam: IOS Press, January. doi:10.3233/978-1-60750-060-5-3.

Sidorenko, Alexey. 2011. Russia: Cyber Security Code of Conduct? *GlobalVoices*, 23. September.

Starr, Stuart H, Daniel Kuehl and Terry Pudas. 2010. Perspectives on Building a Cyber Force Structure. In: *Conference on Cyber Conflict*, ed. Christian Czosseck and Karlis Podins, 163 – 181. Tallinn: CCD COE Publications.

Steigerwald, Douglas, Giovanni Vigna, Christopher Kruegel, Richard Kemmerer, Ryan Abman and Brett Stone-Gross. 2011. The underground economy of fake antivirus software. *eScholarship University of California*.

Stone-Gross, Brett, Thorsten Holz, Gianluca Stringhini and Giovanni Vigna. 2011. The underground economy of spam: A botmaster's perspective of coordinating large-scale spam campaigns. In: *Proceedings of the 4th USENIX conference on Large-scale exploits and emergent threats*. Boston, MA: USENIX Association.

Symantec. 2011. Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually. http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02.

Thonnard, Olivier, Wim Mees and Marc Dacier. 2009. Behavioral Analysis of Zombie Armies. In: *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers. Amsterdam: IOS Press.

Tikk, Eneken. 2009. Why Estonia Did NOT Invoke Article 5. http://www.enekentikk.net/2009/03/why-estonia-did-not-invoke-article-5.html (Accessed: 1. November 2009).

Tikk, Eneken, Kadri Kaska and Liis Vihul. 2010. *International Cyber Incidents: Legal Considerations*. Tallinn: CCD COE Publications.

UK Cabinet Office and Detica Ltd. 2011. The Cost of Cyber Crime. http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime (Accessed: 1. August 2012).

United Nations. 2011. Twelfth United Nations Congress on Crime Prevention and Criminal Justice. *General Assembly 65th session, Agenda item 105*. http://

daccess-dds-ny.un.org/doc/UNDOC/GEN/N10/526/34/PDF/N1052634.pdf?OpenElement (Accessed: 1. March 2012).

Watts, S. 2011. Low-Intensity Computer Network Attack and Self-Defense. *International Law Studies* 87.

Wechsler, B. and R.W. Backoff. 1986. Policy making and administration in state agencies: Strategic management approaches. *Public Administration Review*: 321–327.

White, L.G. 1990. *Implementing policy reforms in LDCs: A strategy for designing and effecting change*. Lynne Rienner Publishers Boulder, Colorado.

Wingfield, TC. 2006. When Is a Cyber Attack an "Armed Attack?": Legal Thresholds for Distinguishing Military Activities in Cyberspace. Potomac Institute for Policy Studies.

Wu, Wei-wen. 2008. A hybrid approach to IT project selection 5, 6.

Young, Richard D. 1995. Perspectives on Strategic Planning in the Public Sector. Institute for Public Service and Policy Research, University of South Carolina.

Ziolkowski, Katharina. 2012. Ius ad bellum in Cyberspace – Some Thoughts on the "Schmitt- Criteria" for Use of Force. In: *2012 4th International Conference on Cyber Conflicts*, ed. Christian Czosseck, Katharina Ziolkowski, and Rain Ottis, 2: Tallinn: CCD COE Publications.

EESTIKEELNE RESÜMEE

Käesolevas resümees võetakse kokku doktoritöö „Küberkonflikti korral kasutatavate robotivõrkude vastase võitlemise riiklike strateegiate hindamine" (i.k „*An Evaluation of State-level Strategies against Botnets in the Context of Cyber Conflict*"), mille eest loodab autor pälvida juhtimisteaduse doktorikraadi.

Käesolev küberjulgeolekut käsitlev teadustöö koondab endasse viis akadeemilist artiklit ning ühendab strateegilise juhtimise ja küberkonfliktide[33] uurimisvaldkonnad.

Uurimustöö eesmärk ning hüpotees

Uurimustöö eesmärk on abistada elektroonilise julgeoleku eest vastutavaid organeid, riiklikke küberjulgeoleku asjatundjaid ning poliitilisi nõuandjaid (eelkõige valitsus- ja sõjaväeringkondades), et tõhustada riigi küberjulgeolekut[34] ja aidata langetada teadlikke otsuseid.

Esitatud uurimustöös keskendutakse ainult robotivõrkudele[35], mis on üks küberkuritegevuse põhilisi vahendeid.

Autor on seisukohal, et robotivõrgud on olulised vahendid kõigi küberkuritegevuse liikide puhul ja nende põhjustatava ohu vähendamiseks kasutusele võetud abinõud aitavad riigi küberjulgeolekut oluliselt suurendada.

Riikide valitsused vajavad oma riigi küberjulgeoleku raamistiku tugevdamiseks terviklikku käsitust, et vähendada robotivõrkude abil toimuvate kuritahtlike rünnakute mõju, ning seetõttu on vaja määratleda ja hinnata võimalikke eri strateegiaid. Sellest lähtuvalt on käesoleva uurimustöö põhiküsimus järgmine:

millised on hiljuti päevakorda tõusnud küberkonfliktide korral kõige paremad strateegilised viisid riigi küberjulgeoleku suurendamiseks robotivõrkude põhjustatava ohu vastu?

---

[33] Küberkonfliktide alane uurimustöö tugineb mitmetele eri valdkondadele, näiteks sõjateadusele (sõjanduse põhimõtete ja strateegia osas), arvutiteadusele (vahendite tehnoloogilise baasi ja küberkonflikti korral kasutatavate meetodite osas), aga ka politoloogiale.

[34] Küberjulgeolek on riigi võime panna vastu küberruumis tema huvide ja omandi vastu suunatud rünnakutele või minimeerida nende rünnakute tagajärgi eelnevalt rakendatud asjakohaste meetmete abil, mida toetavad asjaomased õiguslikud, strateegilised ja korralduslikud raamistikud.

[35] Robotivõrk on levinud pahavara, mis võimaldab saada ilma loata ning loodetavasti ka pideva salajase juurdepääsu suurele hulgale ohvrite arvutisüsteemidele. Selle pahavara põhiline eripära seisneb suutlikkuses ühenduda tema looja rajatud juhtimiskeskuse infrastruktuuriga, mis võimaldab võrguloojal hallata distantsilt kõiki nakatunud arvutisüsteeme, mida kutsutakse robotiteks või *zombideks*. Lõpuks moodustub neist *zombide* võrgustik ehk robotivõrk ning selle loojal on võimalik seda ulatuslikult ära kasutada, viies läbi mitmesuguseid kuritahtlikke tegevusi.

Uurimustöö taust

Tänapäeval on robotivõrgud organiseeritud küberkuritegevuse peamiseks vahendiks ning neid kasutatakse muu hulgas näiteks rämpspostituskampaaniate korraldamiseks ning ettevõtjatelt raha väljapressimiseks, ähvardades neid hajutatud teenusetõkestusega (DDoS)[36] või paigaldades viirusega nakatatud süsteemidesse lunavara (*ransomware*). Robotivõrke kasutatakse sageli ka konfidentsiaalse teabe varastamiseks ettevõtetelt ja üksikisikutelt (Kola 2008; OECD 2008).

Lisaks selliste arengute peamiseks tõukejõuks olevale küberkuritegevusele on ilmnenud veel ka uus oht – üksikisikute või rühmituste korraldatud küberrünnakud. Selliste rünnakute põhjused on peamiselt poliitilised ning sellist tegevust nimetatakse sageli häktivismiks[37] (Denning 2001a; Ottis 2010). Kuna nende rünnakute põhjused on teistsugused, valivad nende korraldajad oma sihtmärke teisiti, eelistades sageli äärmiselt nähtavaid ja peamiselt erasektorisse kuuluvaid ohvreid (Czosseck, Ottis and Talihärm, 2011).

Veel paistab, et ka riigid tunnevad kübervahendite vastu järjest suuremat huvi, et edendada nende abil oma riiklikke huve.

Mõned riigid on robotivõrke väidetavalt juba kasutanud – näiteks ajakirjanduse ja uudisteportaalide tsenseerimiseks nii rahuajal (Pavlyuchenko 2009; Nazario 2009a) kui ka konfliktiolukorras (Tikk, Kaska and Vihul 2010). Robotivõrke kasutatakse ka riigi initsiatiivil toimuvate spionaa¸ijuhtumite puhul ning kõnealused võrgud võimaldavad teadupärast juurdepääsu ka äärmiselt kaitstud sihtmärkidele (GTISC and GTRI 2011). Lisaks kaaluvad mõned riigid väidetavalt võimalust kasutada häktiviste ja küberkuritegevusele keskendunud organisatsioone oma huvide edendamiseks. Riigid pakuvad neile vahendeid, juhatust ja kaitset, ent vastutasuks jäetakse nende hooleks küberrünnakute korraldamine. Riigid eitavad hiljem loomulikult igasugust seost rünnakutega.

Uurimisstrateegia ning metoodika

Käesolev uurimus koosneb viiest erinevast avaldatud uurimusartiklist, milles on käsitletud nelja uurimiseesmärki. Töö kõikide osade puhul on valitud ja kasutatud uurimismeetodeid, mida on vastavate eesmärkide puhul õigustatuks peetud.

---

[36] Hajutatud teenusetõkestus (Distributed Denial of Service ehk DDoS) on küberrünnaku viis, mille käigus saadetakse rünnaku objektiks olevale ühele süsteemile (näiteks e-postiteenuse pakkujale või veebilehele) hulgaliselt päringuid, et see arvukate üheaegsete protsesside tõttu ummistuks. Sellise rünnaku puhul on robotivõrgud eelistatuim vahend.

[37] Häktivism on tehissõna, mis on tuletatud sõnadest aktivist ja häkker. See viitab isikute või rühmituste kuritahtlikule kübertegevusele, mille eesmärk on pigem poliitiliste seisukohtade esitamine kui rahalise kasu saamine (Denning 2001a).

Üldise lähtepunktina kasutati positivistlikku uurimisstrateegiat. Esimese nelja teksti puhul kasutati peamiselt juhtumiuuringuid ja süsteemianalüüsi tehnikaid.

Viiendas osas kasutati mitmetel kriteeriumidel põhinevat otsuselangetamismeetodit nimega DEMATEL (lühend ingliskeelsest fraasist *Decision-Making Trial and Evaluation Laboratory*). Selle meetodi abil analüüsitakse omavahel läbipõimunud tegureid ja mõjusid (näiteks strateegiate kogumit ja selle mõju asjaomasele probleemile), luues neist hierarhilise mõjusüsteemi. Selline lähenemisviis võimaldab töötada asjaomase probleemi jaoks välja hierarhilised lahendused. DEMATEL põhineb graafiteoorial ning seda on alates 1980ndatest aastatest kasutatud edukalt paljudes valdkondades ja tuhandetes uuringutes.

Esimene uurimiseesmärk oli anda parem ülevaade küberkonfliktide eripärast ning 21. sajandi ohtude muutunud pildist, millega peavad arvestama nii riigid kui ka organisatsioonid. Lisaks määratleti kitsas huvivaldkond, millele edaspidi keskenduda – nimelt süsteemide nõrkade külgede osatähtsus ja roll küberkonfliktide eri osalejate vahelises võimuvõitluses. Samuti märgiti käsitletava teemana ära küberrelvade olemuse ja nende eeldatavate uute või ainulaadsete aspektide uurimine.

Sellele küsimusele otsiti vastust **esimeses uurimisartiklis**. Kõigepealt sõnastas autor selles küberrelvade määratluse, misjärel esitati küberrelvade ja konventsionaalsete relvade võrdlus, analüüsides nii nende sarnasusi kui ka erinevusi. Peamiselt keskenduti süsteemide nõrkuste tohutule osatähtsusele, mistõttu töötati artiklis välja ja esitati selline küberkonflikti mudel, mis põhinebki süsteemide nõrkustel. Kõnealune mudel võimaldas muu hulgas analüüsida ka suhteid küberrünnakuvõimeliste toimijate (näiteks riikide) vahel.

Teine uurimiseesmärk oli analüüsida robotivõrkude senist kasutamist küberkonfliktide korral.

Selleks uuris autor hiljuti toimunud küberintsidente, mille puhul kasutati peamiselt robotivõrke, ning seejuures kasutas autor peamiselt andme- ja süsteemikaevandamist. Selle tulemuseks oli **teises artiklis** avaldatud robotivõrkude kasutuskeskne taksonoomia. Erinevalt varasemast tööst ei keskenduta selles ainult tehnoloogilistele aspektidele, vaid terviklik ülevaade antakse ka toimijatest, nende motiividest ja oodatud tulemustest.

Kolmas uurimiseesmärk oli avastada, milliseid ressursse (milliseid oskusi ning kui palju aega ja raha) on vaja selleks, et robotivõrku soetada ja üles seada. Seda võrreldi ka robotivõrkude hävitamiseks vajalike vahenditega.

Mitmete hiljuti hävitatud robotivõrkude (juhtumiuuringud) analüüsi ning eri robotivõrkude struktuuri süvitsi käsitlemise põhjal esitati **kolmandas uurimisartiklis** robotivõrkude klassifikatsioon, mille aluseks võeti võrkude

keerukus. Samuti esitati loetelu robotivõrkude vastu võitlemise kõige levinumatest meetoditest ning selle põhjal tekkis arutelu ressursside üle (aeg, oskused ja raha), mis on vajalikud selleks, et robotivõrke arendada, soetada, kasutada, kaitsta ja hävitada. Arutelus käsitleti piiratud määral ka tutvustatud vastumeetmetega seonduvaid õiguslikke ja eetilisi probleeme.

Seejärel püstitati **neljas uurimiseesmärk**, milleks oli riiklike strateegiate raamistiku väljatöötamine robotivõrkude põhjustatava ohu vähendamiseks, samuti nende strateegiate tõhususe hindamine.

Neljandas trükises sõnastati järeldused Eesti küberjulgeoleku raamistiku kohta pärast 2007. aastal kogetud küberrünnakuid (juhtumiuuring). See, asjaomase kirjanduse läbivaatamine ning osalemine mitmetes rahvusvahelistes töörühmades aitaski autoril välja töötada riigi tasandi strateegilised valikud. Neid omakorda analüüsiti DEMATELi meetodiga, et leida vastus kogu töö uurimisküsimusele. Kõnealuse analüüsi tulemused avaldati **viiendas trükises.**

Peamised järeldused

Esimese ja teise uurimiseesmärgi puhul jõuti järeldusele, et küberrelvade kontseptsioon erineb konventsionaalsete relvade puhul järgitavatest põhimõtetest piisavalt palju, nii et nende puhul ei ole võimalik rakendada konventsionaalsete relvade puhul kasutatavaid tavapäraseid mudeleid.

Samuti selgus, et infotehnoloogiasüsteemide nõrkuste tundmine on muutunud küberkonflikti olukorras strateegiliseks kaubaks. Küberruumis sõltub rünnak ja kaitse otseselt mõlema poole suutlikkusest neid nõrku külgi avastada ja ära kasutada.

Küberkonfliktide uus mudel, mis põhinebki süsteeminõrkustel võimaldas jõuda veel järgmistele järeldustele ja anda seeläbi täiendav panus küberkonfliktide üle toimuvasse arutellu.

Küberrelvi on võimalik hävitada sellega, et kõrvaldatakse viga, mis võimaldas neil mõjule pääseda. Selle meetodi abil saab küberrelvi hävitada küberruumis.
Ratsionaalse käitumise korral ei hävita vea kõrvaldamine ja küberrelva lõhkumine teise osapoole küberkaitse suutlikkust.

Lõpuks leidis kinnitust ka eeldus, et robotivõrkude esialgne roll (olla küberkurjategijatele ebaseaduslikul viisil raha teenimise vahend) on muutunud – nüüd kasutavad seda mitmesugused küberruumis tegutsevad toimijad, kusjuures nende eesmärgid on väga erinevad. Seetõttu peavad nii era- kui ka riigiasutused endale teadvustama, et võivad sattuda robotivõrkude abil korraldatavate rünnakute ohvriteks ning et need rünnakud võivad olla tõsisemad kui tavaline küberkuritegevus.

Kolmanda uurimiseesmärgi puhul leidis kinnitust asjaolu, et isegi olemasoleva tehnoloogia abil on konkreetse robotivõrgu hävitamine organisatsioonilisel tasandil väga raske või isegi võimatu. Selle peamiseks põhjuseks on õiguslikud piirangud ning tõsiasi, et selline töö eeldab ajamahukat analüüsi või ülemaailmselt koordineeritud tegevust.

Kuigi robotivõrke on võimalik hävitada, on selleks vaja asjakohast (juriidilist) luba ning enamasti see puudub. Samuti aeglustab robotivõrkude hävitamispüüdeid vajadus rahvusvahelise koostöö ja kooskõlastamise järele, mistõttu ei ole võimalik probleemile kiirelt reageerida.

Robotivõrkude arendajatel on märkimisväärne edumaa ning olukorra taas kontrolli alla saamiseks tuleb infotehnoloogiaalase julgeoleku valdkonnas lahendada märkimisväärsed probleemid.

Robotivõrkude kasutamine on enamasti lihtne ning nende soetamine on odav; lisaks on robotivõrku lihtne üles seada, mistõttu ei ole nende kasutamisele tõsiseid takistusi.

Neljanda uurimiseesmärgi puhul koostati ning esitati raamistik, mis koosnes kümnest võimalikust riikliku tasandi strateegilisest lahendusest. Nende tulemuslikkust robotivõrkude põhjustatava ohu vähendamisele hinnati DEMATELi meetodi abil, tuginedes empiirilistele andmetele, mis saadi tunnustatud asjatundjate rühmalt, kelle seas oli küberjulgeoleku ja robotivõrkude eksperte, aga ka tööstusalase, valitsusküsimuste ja akadeemilise taustaga inimesi ning tehnika, haldus- ja juriidilise kogemusega inimesi.

Käesoleva teadustöö uurimisküsimuse lahendusena võib läbi viidud uurimistöö põhjal soovitada riikliku küberjulgeoleku suurendamiseks robotivõrkude rünnakute vastu järgmisi strateegiaid.

Esiteks sai kinnitust üldlevinud veendumus, et kõige paljutõotavamad strateegiad on need, mis hõlmavad internetiteenuse pakkujale teatavate kohustuste ja stiimulite kehtestamist.

Teiseks tasub pöörata rohkem tähelepanu küberkindlustusele, tarkvaraarendajate kohustustele ning robotivõrkudega võitlemise algatustele. Nendest strateegiatest räägitakse riikide kontekstis väga harva.

Lisaks määratleti mõistlike valikutena riiklike eesmärgipäraste küberjulgeolekustrateegiate arendamine, kohustuste ja vastutustundliku käitumise stiimulite loomine ka lõppkasutaja jaoks ning rahvusvahelise õiguse jõustamise lepingute sõlmimine. Varemnimetatutega võrreldes ei ole need kolm paraku nii mõjusad.

Viimaks ei ole mõttekas investeerida partnerlusprogrammidesse, teavitus-kampaaniatesse või teadus- ja arendustöö programmidesse (viimane soovitus on siiski üsna piiripealne), kuna need strateegiad ei aita vähendada robotivõrkude põhjustatavat ohtu riiklikule küberjulgeolekule.

Piirangud ja kriitika

Käesolevas uurimustöös keskendutakse ainult robotivõrkude põhjustatud ohule.

Strateegilisi lahendusi hinnati ainult selle järgi, milline on nende eeldatav mõju robotivõrkude põhjustatud ohu korral. Nende rakendamise kulukust või nende kasutamist piiravaid võimalikke takistusi ei arvestatud. Lisaks tunnistab autor, et poliitikakujundajad peavad oma otsuste langetamisel arvestama ka poliitilisi asjaolusid.

Hindamine toimus ka äärmiselt üldistavalt – selle käigus koondati sarnased võimalikud strateegiad suurtesse rühmadesse ja neid hinnatigi selliste rühmadena. Autor pidas seda uurimistöö analüüsietapis asjakohaseks.

Kuigi DEMATELi meetodi kasutamine oli edukas ning selle abil töötati välja vajalik mõjumudel ja hinnati riigi tasandi strateegiaid, osutus see oma käsitusviisi poolest piiratuks.

Välja töötatud mõjumudel koosneb 17 elemendist, mis tähendab, et iga küsitletud ekspert pidi võrdlema ligi 300 paari. Töö mahukuse tõttu reageeriti küsitlustele oodatust loiumalt ning lõpuks osales projektis vaid 11 eksperti.

Sellegipoolest on nad kõik omal alal tunnustatud asjatundjad, kes omavad kogemusi arvukates valdkondades alates tööstusest ning valitsus- ja akadeemilistest ringkondadest ning lõpetades tehnika, halduse ja õigusteadusega. Lõpptulemusena võib uurimustöö tulemusi usaldada, kuna kaasatud asjatundjate hulga tõttu arvestati tulemuste võimaliku ekslikkuse määrast maha faktor suuruses ligikaudu 3,5. See tähendab, et töö järeldused on piisavalt usaldusväärsed.

CURRICULUM VITAE

Personal Information

Name:	Christian Günter Czosseck
Date and place of birth:	16.01.1978, Berlin, Germany
Citizenship:	German
University address:	Estonian Business School, Lauteri 3, 10114 Tallinn, Estonia
Email:	Christian.Czosseck@gmail.com

Education

2010 – 2012	PhD Candidate Estonian Business School
2000 – 2004	Diplm. Inform. (univ.) in Computer Science Universität der Bundeswehr München

Work experience

2008 – 2012	Scientist at the NATO Cooperative Cyber Defence Centre of Excellence
1997 – now	Army officer in the German Armed Forces

Academic activities

Academic Publications:

- Czosseck, C. and Podins, K. 2012. A Vulnerability-Based Model of Cyber Weapons and its Implications for Cyber Conflict. In *Proceedings of the 11th European Conference on Information Warfare and Security*. Laval: Academic Publishing Limited, 198-205.
- Czosseck, C. and Podins, K. 2011. An Usage-Centric Botnet Taxonomy. In *Proceedings of the 10th European Conference on Information Warfare and Security*. Tallinn: Academic Publishing Limited, 65-72.
- Czosseck, C., Klein, G. and Leder, F. 2011. On the Arms Race Around Botnets - Setting Up And Taking Down Botnets. In *Proceedings of the 3rd International Conference on Cyber Conflicts*. Tallinn: CCD COE Publications, 107-120.
- Czosseck, C., Ottis, R., Talihärm, A.-M. 2011. Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security. In *Journal of Cyber Warfare and Terrorism*, 1 (1), 24-34.
- Czosseck, C. 2012. Evaluation of Nation-state Level Botnet Mitigation Strategies Using DEMATEL. In *Proceedings of the 11th European Conference on Information Warfare and Security*. Laval: Academic Publishing Limited, 94-103.

Publication Chair and Editor of the Following Conference Proceedings:

- C. Czosseck and K. Geers. 2009. *The Virtual Battlefield: Perspectives on Cyber Warfare.* IOS Press, Amsterdam.
- C. Czosseck and K. Podins. 2010. *Proceedings of the Conference on Cyber Conflicts 2010.* CCD COE Publications, Tallinn.
- Czosseck, C., Tyugu, E. and Wingfield, T. 2011. *Proceedings of the 3rd International Conference on Cyber Conflicts.* CCD COE Publications, Tallinn.
- Czosseck, C., Ottis, R., Ziolkowski, K. 2012. *Proceedings of the 4th International Conference on Cyber Conflicts.* NATO CCD COE Publications, Tallinn.

Program Committee Members of the Following Conferences:

- 11th European Conference on Information Warfare and Security (ECIW 2012), Laval, France
- International Symposium on Open Source Intelligence & Web Mining (OSING-WM 2012), Odense, Denmark
- 4th International Conference on Cyber Conflicts (CyCon 2012), Tallinn, Estonia
- 3rd International Conference on Cyber Conflicts (ICCC 2011), Tallinn, Estonia


9 789949 929269