Hierarchies in networks. Emerging hybrids of networks and hierarchies for producing Internet security.

Andreas Schmidt

Delft University of Technology

Faculty of Technology, Policy, and Management

a.schmidt at tudelft.nl

Paper prepared fort the edited book *Cyberspace and International Relations. Theory, Prospects and Challenges, e*dited by Jan-Frederik Kremer and Benedikt Müller, 2013 (forthcoming).

The original publication is available at www.springerlink.com.

Abstract

Networked governance is the default modus operandi in Internet governance. Even the provisioning of Internet security heavily relies on non-hierarchical, networked forms of organisation. Responses to a large-scale botnets show the prevalence of networked governance on the Internet and provide insight into its strengths and limitations.

Networked governance can be defined as a semi-permanent, voluntary negotiation system that allows interdependent actors to opt for collaboration or unilateral action in the absence of an overarching authority. This chapter analyses the ability of traditional powerful actors such as state authorities and large enterprises to provide Internet security and exert power in the cyber-domain.

The chapter outlines potential anchor points for traditional powerful actors to introduce more elements of hierarchy and control into Internet security provisioning networks. Empirically, the chapter describes emerging hybrids of networks and hierarchies in Internet security provisioning.

1. Introduction

Empirical research has shown the prevalence of networked governance in Internet security provisioning institutions. (Mueller, Schmidt & Kuerbis, 2013) The characteristics of current Internet security problems, their global distribution of both attacking resources and those needed for responding to security incidents require a networked approach. In recent years, however, discussions on Internet security do no longer only engage technical forums, but also G8 meetings and international conferences of senior policy-makers. Internet security has become a concern of national security politics. One can therefore hypothesize that state authorities attempt to achieve more important, if not pivotal role in Internet security. Given the distributed control over decisive technical resources, states cannot merely incorporate the tasks of existing security networks into the portfolio of their bureaucracies.

The existing international relations literature literature (Eilstrup-Sangiovanni, 2007; Raustiala, 2002; Slaughter, 1997; , 2004) has not adequately explored the interplay of networks and hierarchies in the domain of Internet and information security. Likewise have literatures on networked organisation and security and policing studies so far ignored the issues of governance of the Internet and its security. (Bryden & Caparini, 2006; Krahmann, 2005; , 2010) This chapter is therefore concerned with the question how traditional powerful actors could theoretically and do practically alter existing networked forms of Internet security provisioning.

This chapter is organised as follows. The first part analyses the hierarchies within networks from a theoretical perspective. It starts with a section on models of security provisioning, in which networked security is presented as but one way of providing security. The second section of the theoretical part discusses how networks can be altered by traditional powerful actors to the latter's advantage. The second part of the chapter is devoted to some empirics in Internet security provisioning. The chapter argues that in anti-botnet response endeavours a relatively egalitarian network of actors is replaced by networked approaches with increasingly hierarchical elements. Two subsequent empirical sections depict the arguable rapprochement between national security communities and Internet security communities. The chapter concludes with a call for a more in-depth analysis of both theoretical and empirical aspects of hierarchisation of networks.

2. Security, networks and hierarchies in international relations

2.1.Models of international security

Different degrees in hierarchies in security governance have been a classic topic in the studies of international relations. Starting from the idea of international anarchy, i.e. as unregulated sphere among rivalling, potentially aggressive nation states, international relations theory has come up with several models to explain the absence of war. Prominent ideal-type systems for international security are balance-of-power relations, collective security, hegemonic peace, and international regimes. This list needs to be supplemented by networked security.

Based on the construct of international anarchy, balance-of-power is the first model to provide a secure international sphere, albeit in a precarious manner. In an assumed world, where individual actors, i.e. states, are not restrained and civilized by any institutions means such as global hierarchy, a benevolent hegemon, international cooperation or regimes, states are incentivized to maximise their influence and are even compelled to behave aggressively and therefore increase the insecurity for their peer contenders in the international arena. The ominous international anarchy forces individual states into building up there own defence, response and attack capacities. At best, the capacity build-up results in durable balance of power, in which neither state dares to deploy its forceful means for the fear of a harmful retaliation of the attacked and by-standing actors. Mutually assured destruction is the most vicious form of a stable balance-of-power formation.

Contrasting the balance-of-power model in terms of organisational precision is the collective security model, in which threats for states emerging from other states are mitigated by the establishment of a regional or global authority responsible for protecting international peace. The League of Nations and the United Nations implement a federated variant of this idea. The central version of collective security model has been outlined by Grenville Clark and Louis Sohn in their book *World Peace Through World Law,* a concept of a world government with substantial authority, a kind of super-empowered UN with a substantial executive forces to overcome the governance problem created by the invention of nuclear and hydrogen bombs. (Clark & Sohn, 1958)

Comparable to collective security for its dominant, central forceful entity, a single entity of the international system, a state rather than an international organisations, amasses power second to none, choses to only exert it by and large in benevolent ways and thereby acts as the guarantor of an hopefully just and peaceful existing order. Third states that oppose this order may face the forceful response of the hegemon, while aligned states are protected by the hegemon against attacks from third parties. The price for enjoying this gift of stable order in addition their required support for the hegemon, however is to endure the shortcomings of the existing order. The "benevolent hegemon"—a role frequently attributed to the United States after the end of US-Soviet conflict—ensures global security and prosperity as global public goods. (Mandelbaum, 2006; Nye, 1990) Using the concepts of institutional economic theory, a state's hegemony establishes a "hierarchy between polities [that] reduces transaction costs and mitigates opportunism" (Lake, 2009, p. 275).

The fourth fundamental way to ensure a peaceful international order mixes some of the characteristics of the previously described approaches. Lacking stable orders provided by the models of collective security or hegemonic peace, states can still reduce their mutual distrust that could eventually result in an arms race and thus spiralling societal cost for security provisioning. By engaging in international cooperation and establishing international regimes and norms, states can manage to balance their security interests, reduce mutual distrust and establish an international order that doesn't resemble a zero-sum game. For many international issues, the various forms of international regimes have are the default organisational form of international problem solving.

Resembling international regimes, networks in various forms have entered the sphere of global politics as an organisational form. The concept of transgovernmental networks reflects the widening and deepening of international collaboration and intensification of communication at medium and lower level of hierarchies in national bureaucracies. These TGNs manage to produce outcomes beneficial to the states involved. During the last decade, security and policing studies have observed a diversification of how security is provided, away from the state as the sole provider of public security towards a system where the state is supplemented by private actors such as security services and mercenaries. In national security circles, the term "networked security" refers to "loose institutional arrangements and non-hierarchical structures of information exchange" (Gruszczak, 2008) that are established e.g. in in anti-terrorism activities or to re-establish security in former failed state such as Afghanistan. (Jung, 2009) However, the idea of networked governance goes beyond the idea of networks as a governmental tool.

In practice, Internet security is provided in a highly networked way. Anarchy on the Internet has quite likely never existed. Content distributed by it may have been unregulated for while, but the technical integrity and functionality has been ensured by a community of technical experts ever since these risks have become obvious. This collaboration has resulted in a kind of distributed, bottom-up collective security provisioning. As the previous sections have shown, this model is challenged in a number of was.

So far, there is no established and globally accepted cyber hegemon. Not an act to foster cyber-peace, the US has with its apparent involvement in the Stuxnet attacks showcased how attacks on ICT systems with ICT systems can be used in international conflicts to coerce opponent states. On a regional level, the Russia might have attempted similar outcomes with its likely involvement in the cyberattacks on Estonia in 2007 and on Georgia a year later. The cyberattacks on Iran could benevolently be interpreted as a move forward towards cyber hegemony, which would perpetuate the military dominance of the US from the physical to the digital world. Hegemonic cyber-peace would describe a world in which no country would dare to launch cyber attacks against third countries for the fear of retaliation by the hegemon, who would be legitimized by an adapted international law and optionally authorized by an international body. This model assumes that cyberspace is a potential place for interstate conflicts and to exchange coercive means to bring down opponents. It is arguable whether such cyber hegemony will come to exist in the near future. Nye argues that the US most likely has the most sophisticated attack capabilities, but is on the other hand more vulnerable to cyber attacks than other countries. (Nye, 2011a)

There is no collective security organisation akin to the UN or the OECD to balance national security interests in cybersecurity. Warnings about an imminent cyber-arms-race date back almost as long into the past as prophecies of doom brought by forthcoming digital Pearl Harbours, which usually also served as a call for a nation, usually the US, to start or speed up the build-up of its cyber defence and attack capabilities. (Brito & Watkins, 2011; Deibert, 2010; Minkwitz & Schöfbänker, 2000) Apparently, these early warnings for a cyber-arms race have been to no avail. Nations states are in the midst of an "[accelerating] global cyber arms race",

according to Cybercom's director of intelligence. (Benitez, 2012) Founder and CEO of AV and security company Kaspersky Lab, Evgeny Kaspersky, has called for a new dedicated organisation. The "ÒInternational Cyber-Security Organisation" should act as an "independent global platform for international cooperation and treaties on non-usage of cyber-weapons, and cyber-security regulations for critical infrastructures." ("CeBIT 2012: Eugene Kaspersky calls for international cyber-security organisation," 2012)

2.2.Hierarchies in networked security

The responses to Internet security rely on networks. The question about which forms of organisation emerge when ideal-type forms such as networks and hierarchies merge has been raised by authors such as Steven Weber or David Ronfeldt.Nevertheless, existing networks literature doesn't provide a detailed look on the relationship between traditional powerful actors, such as states and large corporations, and networked governance in transnational forms of organisation. Likewise, IR literature that embraces networked governance still focuses on governmental and state authorities. (Mueller et al., 2013) A number of key questions, e.g. whether the networked approach and the decreased importance of states in Internet security is temporary or permanent, have therefore remained unanswered. This article therefore aims at analysing the relations between hierarchies and networks within the networked approach by a) developing a model of how traditional powerful actors theoretically interact with inevitable security networks and alter them to their advantage and b) analyse recent developments in Internet security and their effect on the qualities of Internet security provisioning networks.

Hierarchies can be defined "as a continuum on which one actor has more or less political authority over other actors." (Lake, 2009, p. 264) This more political, less sociological conceptualization is closely related to the idea of political authority, which "is most simply understood as rightful or legitimate rule" akin to what can be found within firms, governmental bureaucracies or between governments and citizens. (Lake, 2009, p. 265) The conceptual lines between political authority and political power are blurry, making them all closely related. Joseph Nye has recently linked power to "behavioural outcomes", defining power as the ability to achieve preferred outcomes by affecting others ("domain") on certain areas ("scope") by coercion, reward, or attraction ("means"). (Nye, 2011b, p. 21) Despite similarities, hierarchy is not synonymous to power, at least not with Lake's conceptualisation. The difference is that hierarchy refers to an organisational structure that is characterized by institutionalized asymmetric power-relationships between higher positions in the hierarchies and those at lower regions in the hierarchy; in addition, this ability to achieve preferred outcome is deemed legitimate.

There are a number of reasons for a nation state or a national government to alter existing power relations. Incentives for creating a hierarchy could either be nurtured by discontent with the outcomes or efficiencies of a given security provisioning institutions; large corporations might use a less equal network to achieve results suit their interests better. Hierarchies are a way to decrease transactions costs with a certain institutions. Next to this efficiency or effectiveness argument, establishing hierarchy can be seen as the means of an actor to create greater influence

on a domain. Much akin to their ability to print money via their central banks, states can create authority, hierarchy and thus power by printing laws, at least in domestic affairs. Major schools of international relations state that states seek or at least would favour to improve their relative power status. With the emergence of security networks and the inevitability of the networked approach in Internet security, states need to react to named institutions that tend to undermine the traditional capacities of states in security governance.

For a nation state that seeks to hierarchify existing global networked security provisioning institutions, there are two ways to achieve this. First, states can alter existing governance networks in a way that grants them more influence or power over other actors.In opposition to earlier normative interpretations of networks as more egalitarian structures, networks can very well have asymmetrically distributed power structures among its members. (Kahler, 2009) In addition, contrary to initial beliefs, open source software and similar projects for distributed production of intangible goods are now known for substantial levels of hierarchy and authority. (Dafermos, 2012; Weber, 2004) Authority in these open source production networks has been established by needs for increasing efficiency, ensuring quality, streamlining internal communication and similar means to reduce transaction costs. (Dafermos, 2012; Weber, 2004)

Network theory provides the recipes for actors willing to increase their influence within networks. The centrality of an actor, the number, density and intensity of connections of a network node, e.g. facilitated by seizing a first-mover advantage (Wong & Lake, 2009), decide over its power status within the network. This common finding of network studies applies to states in international networks as well. (Slaughter, 2009, p. 112) Accordingly, her recommendation for US policy is to increase its "capacity for connection, rather the splendid isolation or hegemonic domination" (Slaughter, 2009, p. 113). It doesn't go much beyond these high-level recommendations, though, just as one would expect with an *Foreign Affairs* article.

An obvious prerequisite to gain influence in networks is to be part of them at first. Traditional powerful actors embed themselves into the previous distributed networked model. This has been happening in the cybercrime area and with police forces and law enforcement. In addition, we have also seen first attempts by military and intelligence organisation to liaise with these InternetInternet security communities. The same holds true for large corporations that required the support of the Internet security community after attacks on their systems. To give an example, Siemens has increased its visibility and information sharing with ICT security communities as a result of Stuxnet, and Apple has for the first time participated in major conferences of the security community, abandoning its usual go-it-alone procedure after a year with several exposed vulnerabilities of its operation system platform. (Jackson Higgins, 2012a; , 2012b)

Once actors are a node in Internet security networks, they can start influencing the way these networks operate and thus in the long run alter existing networked security governance models. New combinations of hierarchy and networked approaches are to emerge. An example is the replacement of more egalitarian types of collaboration such as peer-production with hierarchical forms of social production such as crowdsourcing. Malware reverse engineering, a necessity in the response to any major attack on ICT systems, can be co-produced, shared and discussed

openly among experts on their security mailing lists. In the crowdsourced variant, a security company would request for input and attempt to create their own contributory network. The difference between open community-based production and crowdsourcing is that the terms of collaboration and production are defined by the platform owner and crowdsourcing party.

Crowdsourcing is but one example of how existing collaborative networks can be altered by actors. Theoretically, any of the defining characteristics of networks can be adjusted and thereby the nature of the network. Networks differ from hierarchies by their different permeability for membership candidates, a more flat and decentralised organisational structure, low degree of legalisation, trust as the ultimate glue between members, a consensus-oriented decision making process, fast and direct flows of communication, and lower set-up costs and time. Furthermore, as empirical accounts of the Conficker response or the Estonian cyberattacks have shown, security incident response networks actually resemble communities that slightly differ from ideal-type networks and come with a unique mix of access criteria, vetting of membership candidates, conflict resolution, decision making, ownership of shared information, and access to community outcomes.

The following table illustrates the differences among hierarchies and networks for a number of criteria.

criteria	network	hierarchy
membership	more permeable (less so for security networks)	less permeably
structure	decentralised, flat; elements of internal authority	centralised, hierarchical
legalisation	low	high
unit relations	trust-based (in sec comm. trust is based on keeping rules)	rule-based
scope	narrow	broad
decision making	consensus; slow, complicated; frequent renegotiation	few; fast

communication	fast, efficient; ineffective for repetitive tasks, competing agendas	slow, constrained, complicated
scalability	high (low for security networks)	
set-up costs	low; hardly no overhead; (medium for trust-based security networks)	high
set-up time	low (moderated for trust building)	high
adaptability	high	low

The table only depicts ideal types of network and hierarchies. For real-world examples, the characteristics of these criteria of networks and hierarchies might differ. In the case of Internet security response networks, membership and scalability differ form ordinary networks. individuals with certain functional roles ("with something to bring in").

Response activities are usually driven by distinctive communities or even ad-hoc groups, whose members are part of a wider security network. Instead of altering the norms of existing security communities—communities are cohesive and densely connected nodes (Porter, Onnela & Mucha, 2009, p. 1086)—, hierarchical organisations could try to set up new communities within security networks that follow rules favourable to their own goals. These rules can be enforced by market pressure, rule of law or other leverages. Such altered communities can exist in parallel to existing ones that are characterised by more traditional security community governance norms. Thereby, a national security organisation could more easily control membership and access criteria and other important criteria. Presumably highly important for national security organisations is the proper vetting of the member base. While technology-oriented mailing-list-based communities don't discriminate nationality, those dedicated to national security issues could do so more likely.

The second fundamental strategy is to decrease the importance of existing security provisioning networks. Fundamental strategies to achieve this are the creation of new response technologies, alternative technical and political response institutions.

The current state of technology requires a highly decentralized, if not distributed approach. Awareness about the current state of the Internet, the attacks going on, the malware flooding around, require distributed monitoring of networks. Since the emergence of botnet in the early-mid 2000s, capacities to detect and monitor botnets have been increased. So called honeynets or

honeypots installed at different segments on the Internet by different parties, give insight into the malware floating around the Internet; appliances installed in the facilities of Internet service and backend providers analyse network traffic and watch out for suspicious patterns not only within single networks, but on the Internet worldwide; the ever close connection and increasing data exchange with operating systems running on end users' machines, allows OS vendors to analyse Internet traffic and to detect malicious content. So far however, these intermediating traffic analysis systems are not controlled by states, let alone a single state. A technological innovation that would support the state's role would first of all decrease the reliance on distributed input from technical experts around the world and allow for a more centralised form of monitoring and problem detection. Once a certain degree of centralisation is achieved, a state would have more hierarchical counterparts whose behaviour could be incentivised to ensure outcomes in the state's favour.

The importance of technological response networks can also be reduced by establishing non-technical response institutions to prevent security incidents in the first place, such as deterrence or the establishment of international norms such as state responsibility. The question whether deterrence can be applied to the world of information technology has been a standard topic of Internet security literature. While in the beginning, authors tended to deny the transferability of deterrence mainly because of the alleged impossibility to identify attacks—the so-called attribution problem—, the idea to codify more extensive obligations for states to assist each other during incidents has recently gained popularity among pundits. Cold-war wisdom comes to rescue here. Other than frequently stated, the attribution problem, the problem to identify the perpetrators of an attack beyond any doubt, doesn't exclude the build-up of plausible, deterring threats. (Healey, 2012; Nye, 2011a) "Active response"—a popular topic in recent security discourses—might actually result in an upping of existing deterrence, such as the capability to damage a state's reputation that is allegedly very likely responsible for the attacks. (Nye, 2011a, pp. 33-34)

3. Hierarchies in botnet responses

While the previous sections have delved into the theoretical perspectives of hierarchies within networks, the following sections discuss some empirical developments in the area of Internet security provisioning. This section starts with a look at the response to the Conficker botnet. Botnets are widely known for their role as a facilitator spam, cybercrime and DDoS attacks. In late 2008, a particularly large botnet plagued networks and computers worldwide. Even more remarkable than the sophisticated attack techniques used by the botnet's malware, were the efforts by networks of network security experts to respond to or at least mitigate the problem this botnet posed. The response to the Conficker botnet heavily relied on networked governance in what could pose as an ideal-type form of security provisioning by a networked of relatively equal players and without significant involvement of state authorities. (Mueller et al., 2013; Schmidt, 2012)

The response to the Estonian cyberattacks in 2007 relied on a similar bottom-up approach with

little involvement of corporate and state hierarchies. (Schmidt, 2013) Hence, "at least at that moment of Internet history, states played hardly any role in responding to attacks on an infrastructure so densely interwoven into many societal practices, either at the operational or governance level." (Mueller et al., 2013) However, the response to the Conficker botnet was but one ad-hoc effort to mitigate the impact of a botnet, more were to come and a few among them included a few more hierarchical elements than the Conficker response. Since 2009, much of the organisational design of the anti-Conficker approach has been reused in other anti-botnet endeavours. In general, we see states attaching themselves to these networks of operators and technical experts and taking roles of varying prominence in these networks. US law enforcement has been particular keen to link up to these technical communities and vice versa. Response activities to post-Conficker botnets such as the DNS Changer scam (von Eitzen, 2011), the BredoLab (Schwartz, 2010), Mariposa (Kolakowski, 2010; Sully & Thompson, 2010) and the ZeuS botnets (Lennon, 2012) are characterised by an increased role of law enforcement agencies.

The DNS Charger malware was first discovered in 2007. The malware intercepts DNS requests made by other software on its host computer and redirects users to illegitimate websites controlled by the DNS Charger gang, where web ads would be served to the visitors. The malware had infected some 4M computers, and served their users with faked ads from their 350,000 servers, leaving $14M advertisement costs for their victims. (FBI New York Field Office, 2011) The DNS Changer Working Group (DCWG) botnet included many of the players of the Conficker Working Group, complemented by a significant role for the FBI and the National Cyber-Forensics & Training Alliance, a non-profit partnership between law enforcement and technical experts from industry and academia. In November 2011, FBI announced its "Operation Ghost Click", which would lead to the seizure of a block of IPv4 addresses by Dutch prosecution authorities on behalf of the FBI. Eventually, a court order temporarily transferred operational control of the domain names used by the DNS Charger gang to one of DCWG's members, the Internet Systems Consortium (ISC). This transfer allowed the DCWG to inform users that their machines had been infected. Other than the Conficker response, the work of the DCWG led to the arrests of 6 Estonians and 1 Russian. (FBI New York Field Office, 2011; Forward-Looking Threat Research Team, 2012)

Bredolab was a significant botnet comprising millions of infected machines until it was dismantled in late 2010. After a weeks-long investigation, Dutch police and prosecution ordered the take down of the command-and-control servers of the Bredolab botnet in October 2010. The technical analysis and operations were seemingly performed by Govcert, Dutch IT security company Fox-IT and the Internet hoster Leaseweb. Police claimed 30M computers according to the press release issued by the Dutch police Team hight Tech Crime (Openbaar Ministerie, 2010), however, these numbers were more likely much lower. The investigation into Bredolab, called "Operation Tolling", was part of a wider campaign against botnets by Dutch authorities. The Dutch police even had a dedicated communication team with the goal to raise awareness of the botnet problem in the wider public.(Korps Landelijke Politiediensten, 2011) Law scholars, civil society Internet activists and AV vendors criticised the police for taking over infected machines and sending warning messages to their users.

In late 2010, the Mariposa botnet was brought down by a joint effort of Canadian, Spanish, and US security experts collaborating with the FBI and Guardia Civil. (Larraz, 2010; Leyden, 2010; Sinha, Boukhtouta, Belarde & Debbabi, 2010) One of the largest botnets ever, Mariposa consisted of 11m unique IP addresses over the entire lifespan of the botnet and was used for the usual cybercrime variants, including spam, theft of online credentials, and DDoS attacks. (Sully & Thompson, 2010) To respond to the Mariposa botnet, the technical community again formed an ad-hoc working group that to a large extent resembled the Conficker Working Group. The working group was initiated by a small Canadian anti-botnet solution vendor Defence Intelligence and supplemented by Spanish security company Panda Security, network company Neustar, Directi, and by academics of Georgia Tech's Information Security Center, plus a number of unnamed researchers from other institutions. (Sully & Thompson, 2010, p. 10) As Defence Intelligence later frankly admitted, they first aimed at turning its detection and analysis of the Mariposa malware into a marketing success. In the course of the response they learned, that turning a collective effort into a unilateral marketing success undermines the mutual trust that is required for such international anti-botnet campaigns. DI seemingly wanted to steer the group, but lacked the authority to actually enforce the direction it wanted the group to head into. (Sully & Thompson, 2010, p. 16) Eventually, the botnet was brought down, the botherders and the developer of the underlying Mariposa software kit arrested.

In spring 2012, a working group lead by Microsoft initiated the seizure of the, as Microsoft stated it, "Zeus botnet". (Boscovich, 2012) The consortium was lead by Microsoft's Digital Crimes Unit and supported by the company's Malware Protection Center, the US Financial Services Information Sharing and Analysis Center (FS-ISAC) and Electronic Payments Association (NACHA), ICT security company Kyrus Tech Inc, which was responsible for the malware analysis (Krebs, 2012), and AV vendor F-Secure. Additional intelligence came from global ISPs and CERTs. (Cf. Boscovich, 2012) The consortium eventually dismantled a botnet created with Zeus-malware variants Ice-IX and SpyEye. (Bijl, 2012) Zeus is a malware toolkit, a type of software that miscreants can use to create their own malware and with which they can then create their own botnets. (Macdonald & Manky, 2010) Microsoft's stated primary goal was to not bring down the botnet entirely, but to primarily "inflict costs on cybercriminals". These goals conflicted with some of the other network partners with more perseverance and an interest in the permanent take down. Some of them e.g. had build up hidden online personae that were then exposed by the texts in the law suit filing. Analyst and blogger Rik Ferguson of AV company Trendmicro pointed at the importance of close collaboration with law enforcement and stated successful collaboration with LE agency requires more time, but leads to more sustainable results. (Ferguson, 2012) Ferguson blames Microsoft for prematurely exposing identities of perpetrators, thereby severely harming due legal process and the ability to prosecute perpetrators. Dutch ICT security company Fox-IT blamed Microsoft outright of obstructing criminal investigations. (Bijl, 2012; de Natris, 2012) Fox-IT labelled Microsoft's "Operation B71" as ineffective, short-sighted, marketing-oriented and as a blow to the established trust and effectiveness of the security community by snubbing the community of using shared information only with the agreement of the sharer.

In general, the networked approach in Internet security mirrors a general trend in policing and security that has been observed in the last two decades, in which the statal monopoly of force has been riddled in a number of areas. (Kempa, Carrier, Wood & Shearing, 1999; Krahmann, 2005) State authorities have been relegated to a marginal position or even a virtually non-existing role in the Conficker case. However, the response activities after Conficker appear to have more hierarchical elements than the combined efforts of Conficker Working Group and the global security communities and networks. Reflecting changes in the way how actors responded to Internet security incidents, the altered, more prominent roles of both law enforcement and large companies comes to mind. In the response endeavours after Conficker, state authorities have increasingly embedded themselves into existing response communities of the larger Internet security network. Likewise, large companies have tried to push egalitarian rules of the security community and to take a leading role in these response communities. In the Bredolab case, the Dutch High Tech Crime Team took the driving seat. The most significant changes from an organisational prospective were the takedowns of the Bredolab botnet under the guidance of the Dutch police and Microsoft's blatant breach of community code in the 'ZeuS botnet' takedowns. The number of cases certainly is too small to see a statistical trend in these developments. Qualitatively, it is however significant that some embedded player attempt to design botnet response activities in their own way.

In terms of rhetoric, the rollback of Internet security governance by states is even more ahead. A number of influential policy-makers have called for a built-up of contingency capabilities that would provide public authorities and national security institutions with far-reaching capabilities in the area of surveillance, identification and communication traffic control. (Gorman & Barnes, 2011; McConnell, 2010; Pear, 2012) Unsurprisingly, such political rhetoric makes its way into actual Internet security policies and operations in other, non-botnet areas of Internet security as the subsequent sections demonstrate.

4. Rapprochement of national security and technical security communities

4.1.The Estonian Cyber Defence League

Incumbent security institutions such as police, military and intelligence agencies have stood on the side-lines of response efforts against infrastructural security incidents for years. Their contribution to mitigating large-scale Internet security incidents such as the Conficker botnet or the Estonian cyber attacks was virtually non-existent. Nevertheless, governments have started to grasp the importance of the global Internet security community for re-establishing the availability and functionality of common Internet-based services in times of attacks. With Internet security moving up to the very top of national political agendas, these communities are slowly becoming a focal point of national cyber-security politics. Estonia spearheaded this trend right after it had lived through its 2007 cyberattacks. One of the consequences the Estonian government drew from the incident was to establish the Estonian Cyber Defence League (CDL).

Far from setting up an operational team of hackers or cyber warriors, the Cyber Defence League creates an organisational umbrella for the otherwise loosely coupled community of technical experts that had saved the Estonian Internet infrastructure from a full-fledged halt in April and May 2007. While the Estonian ministry of defence issued sharp rhetoric after the attacks, its contribution to solving this "national security situation" was marginal. It took days until the ministry of defence asked the technical community for a thorough briefing on the situation. In the later days, its task was to exchange information with its foreign peers in Western embassies and capitals. Political circles cried "cyberwar" (Poulsen, 2007), but couldn't do anything, while technical circles cooly managed the situation and mitigated the attacks (Davis, 2007; Schmidt, 2013).

Not everything was perfect with the response of the Estonian technical community. For one, the Estonian technical community wasn't appropriately connected to the international networking community, which was needed to mitigate the DDoS attacks. Secondly, the information and communication within the Estonian community was highly centralised and lacking back-up capacities. Had the attackers managed to knock off the central node, the Estonian CERT, the Estonian defence activities would likely have slumped down very soon. Third, high-level members of Estonian ministries were aware of strong indications that Russian communities were planning DDoS attacks on Estonian Internet services. (Gomez, 2012) Such early warning could have been used to reach out to the Russian government and request assistance to hinder these attacks from happening in the first place. However, the early warning got stuck somewhere in-between the lower and highest ranks of the Estonian ministries. (Schmidt, 2013)

The CDL establishes an organisational link between Estonia's civil technical community and it's military establishment. After the 2007 attacks, the community of Estonian Internet security experts was formalised under the umbrella of the Cyber Defence League in 2009. In 2011, the CDL became part of the Estonian Defence League (DL) as its Cyber Defence Unit. (Estonian Ministry of Defence, 2011) The Estonian Defence League is an 11,000 persons, all-volunteer paramilitary defence organisation armed with mostly machine guns and antitank weapons. The Defence League was set up after World War I as a response to frequent occupations in the Estonian history and it's therefore aimed to guarantee national sovereignty. The commander of the DL is appointed by leading Estonian militaries. ("Estonian Defence League," 2010)

The CDL does not act by itself as an independent, authoritative force. If If the CDL wanted to, it would have to overrule the links between its technical members and their respective employers or affiliated organisations and break the legal employer-employee relationship. The CDL's members, who are partly employees of Estonian private companies, would be drafted and had to implement orders of CDL leadership in their employers' infrastructure. Instead, the CDL acts as "coordinator and supervisor of the activity of volunteer cyber protection specialists" and it "would not provide counterforce itself, but would instead act only in an advisory capacity." (Estonian Ministry of Defence, 2011) The civilian side of CDL's ambiguous character is represented by its very leadership. The members of the CDL are lead by the same person that also supervises the Estonian CERT and reports to the ministry of economic affairs.

The rationale behind the foundation of the CDL is to "harness… the skills and resources of

security specialists and enthusiasts for a constructive purpose." (Ottis, 2010) Of the shortcomings of the 2007 response model described above, the organisational form of the Cyber Defence League mainly addresses the vulnerability of the response organisation, in which CERT EE held a central, indispensable role. But not everyone who participated in the 2007 response efforts was pleased with the paramilitarisation of the Estonian Internet security community, and preferred to not take part in the CDL. The informal beer-and-sauna protocol has been supplemented by paramilitary traditions. Volunteers dedicate their efforts no longer only to "keep the Internet secure"—a frequently mentioned motivation of contributors to the Conficker response in interviews with the author— , but also to help their respective homelands. Internet security has become a national cause.

4.2.Developments in the U.S.

The developments in Estonian have not gone unnoticed by those who perceive ICT insecurity as a potential threat for national security. In the US, there have likewise been attempts to establish technical communities and gather security enthusiasts for the national cause. The importance of technical communities is increasingly recognized by national security circles. (Gomez, 2012; Klimburg, 2011; Lawson & Gehl, 2011) The Estonian CDL model, however, is built on institutional, cultural, and historical ground unique to Estonia. In order to achieve an "integrated national cyber capability", Alexander Klimburg argues, these technical experts, if not coerced or co-opted, "must be motivated to cooperate with government aims", and mutual trust needed to be build up among them and governments. (Klimburg, 2011, p. 55) "Mobilising cyber power", as his article is titled, requires the collaboration of these technical experts. Indeed, infrastructural Internet security requires support of private actors responsible for or operating the various technical systems that eventually make up the global network of networks. (Schmidt, 2012)

Some of these technical experts have been influenced, if not deeply rooted in what is commonly labelled as Californian ideology, which traditionally is sceptical of governmental authorities. Foreign policy strategists in Washington have faced the need for Silicon Valley's cooperation with the US government once before. New York Times columnist Thomas Friedman expressed the scepticism of U.S. foreign policy circles towards Silicon Valley's then apolitical stance: "There is a disturbing complacency here toward Washington, government and even the nation. There is no geography in Silicon Valley, or geopolitics." (Friedman, 1998) A couple of years later, major player of the US IT industry and traditional US security organisations had joined forces. The "War on Terror" following the 9/11 attack lead to numerous task forces pondering ways to exploit information technology to uncover terrorist networks and their activities. The IT industry had every economic incentive to support its alignment with governments and the ubiquitous use of ICT for national security purposes. (American Civil Liberties Union, 2004, pp. 27-29)

The challenge for national security circles this time however is not to align mere companies, a task that could be solved with ease by a proven mix of rewarding and sanctioning incentives such as governmental purchasing power and anti-trust or tax investigations. In the case of Internet

security, the indispensable actor required by national governments to achieve their national security goals are the networks of security experts, not only companies. Internet security communities usually comprise individual experts dedicated to certain technologies, Internet services, or problem-specific ad-hoc task forces. These individual experts happen to exchange information via access-restricted mailing lists and collaborate, driven by their individual motivation, usually with company backing or at least connivance.

There are historic examples how to include volunteering individuals into an overall national undertaking. Again, the post-9/11 policies provide illustrative examples. Organized watch programmes and citizen awareness campaigns aimed at balancing governmental lack of sensors to detect potential terror suspects,The idea of recruiting informants from specific sectors with broad access to specific parts of individuals' lives gained a foothold in Washington soon after 9/11. The idea behind planned programs like 'Citizen Corps" or the "ÒTerrorism Information and Prevention System" was to get individuals "directly involved in homeland defense." (American Civil Liberties Union, 2004, p. 4) Using a term that was only coined more recently, these programs aimed at crowdsourcing the monitoring of human traffic in societal systems with the results being appropriated by the platform owners, i.e. national security organisations.

Recent developments suggest that the existing security community landscape is being altered by several policy approaches. It isn't obvious, however, whether they are driven by an underlying strategy or are the result of incidental policy projects in different branches and levels of the US administration. An example of such a newly formed network is the Cyber Security Forum Initiative (CSFI). CSFI is a the result of a private initiative, and incorporated as a US non-profit organisation. The Forum, which appears to have close links to US military, aims at educating the US military on cyber warfare and facilitating collaboration and information sharing inside government, military, law-enforcement and industry. While it is a "volunteer group" (Klimburg, 2011) just like the Conficker Working Group, it differs from the widespread type of mailing-list-based Internet security groups in important aspects. Different from these mailings-list-based communities, thorough vetting is no prerequisite for basic membership of CSFI (only for specific projects of the initiative), nor is active contribution required to remain part of the group. This allows CSFI to gather some "5000 Cyber Security and Cyber Warfare professionals", which are, inconceivable for tradition operational-security groups, managed via the LinkedIn social network. Another characteristic of CSFI is its close cooperation with military organisations, exemplified by frequent postings for jobs usually requiring US clearances and related to US military, a joint recruitment sessions with NATO Cooperative Cyber Defence Centre of Excellence , and a dedicated "cyber-warfare division".

While CSFI is private initiative, the second example of changes of relations between states and security communities is more obvious. DARPA's Cyber Fast Track program signifies a departure from usual bureaucratic governmental contracting. The program, directed by former hacker Peiter Zatko, grants funding for short, fixed-price projects to individual researchers and entrepreneurs in the security community. The stated primary goal of this project is to create useful knowledge for the security community. Such funding and collaboration might well alter or ensure the perception of the Pentagon as a trustworthy organisation in the security community.

In the long run, such programs might help to shape political mentalities and dispositions in the information security community. Mentalities among members of the ICT security community can determine whether ICT-based national security incidents are played out along the interests of national security communities or not.

From the perspective of those concerned with ICT-related aspects of national security, the geopolitical implications of the activities of security industry requires need to concern. Publicly, these concerns have so far only been shared in journalistic outlets, however by journalists apparently well connected with Washington's political cyber-security establishment. In a piece that was published in several online subsidiaries of IDG publishing house, Jeff Bardin, Chief Intelligence Office of security company Treadstone 71, accused US security companies for their arguably treacherous support in dismantling "cyber-weaponry" such as Stuxnet, Flame, Duqu, or Gauss, directed at Iran, an "enemy and well-defined adversary" of the U.S. In addition, Bardin finger-pointed at Russian citizen Evgeny Kaspersky, founder and CEO of London-based AV and security company Kaspersky for his alleged loyalty and proximity to the Kremlin. His ongoing loyalty would root in his former affiliation with Russian intelligence agency FSB and would still be visibly by his AV company's exclusive interest in US-originating malware, while ignoring cyber-weaponry developed in his home country. (Bardin, 2012) Such a nationalistic stance on malware analysis was first seen in Wired magazine, where Noah Shachtman, a long-standing and usually sober observer of information security issues (Shachtman, 2011), raised questions about the links of Kaspersky to the Kremlin. (Shachtman, 2012) Wired repeated its allegations against Evgeny Kaspersky by adding him to the list of "Wired's Most Dangerous". Such rumor-based reporting and shaming of actors with possibly lacking loyalty to US-security interests might well shape the stance of members of individuals and companies in the IT security community. Naming and shaming of unwanted actors is a proven and one of the harshest means to alter the behaviour of another actor in a networks and communities without organisational hierarchies.

5. Conclusion

Actors can reply to technological changes that threaten to erode their previous power resources. Brenden Kuerbis doctoral thesis (Kuerbis, 2011) has highlighted how new security technologies "can alter power relations and economic dependencies among stakeholders". (Kuerbis & Mueller, 2011, p. 125) This chapter has aimed at understanding possibly ways for traditional powerful actors to interact with Internet security networks and alter them to their advantage both theoretically and empirically. The motivation for this has not been to provide an early draft of "il Internet security principe", but to provide a tool to better analyse ongoing developments in the field of Internet security and the role of the security community therein from a power perspective.

As a first facet of the analysis, this article first related networked security to other ideal-type models of security provisioning in the international sphere. The characteristic of Internet security is its reliance on the networked approach. Previous ways to provide security as described in the

section Models of international security don't apply to Internet security. There is neither cyber hegemony, nor collective cyber security, or cyber anarchy. Internet security instead is provided predominantly in a networked approach. Within such networked approaches, governments and large corporations can alter networks in various ways to make them more amenable to their interests. In general, these actors can theoretically aim at altering any of the characteristics that define networks that are more egalitarian or try to reduce the importance or even replace these networks by altering the underlying technologies, reduce the importance of established security response communities or replace them with more hierarchical communities.

In the second part of the chapter, the analysis of networked security provisioning in the Conficker case has shown that the currently predominant organisational form for Internet security provisioning is based on networked governance. Response to Internet security incidents largely relies on the contribution of a global community of technical experts with affiliations to various sectors and of law enforcement agencies. However, Conficker's governance model with its relatively levelled power structure appears to be increasingly replaced by a form of networked governance in which states and governments have a greater say. Activities of Developments in the U.S. with close links to them in the national security communities indicate that U.S. authorities are aware of their dependence on these technical communities and aim for a greater role within these networks.

The empirical data presented in the second half of this chapter is certainly not rigidly selected and therefore only provides indications that allow to build the hypothesis that a hierarchisation within networked production of Internet security is underway. To actually prove such a thesis requires a more elaborated theoretical model and, even more so, more rigid data selection, collection and analysis. In our previous paper we have already stipulated the importance to better understand the networked organisational form as the basis for Internet governance and its contribution to growth, resilience of transnational communications. (Mueller et al., 2013) The forces and developments in the field of Internet security highlight the necessity to better understand the intersection of networks and hierarchies or rather the effects that powerful hierarchies and interested market forces have on the networked governance approach.

Bibliography

American Civil Liberties Union (2004, August). The surveillance-industrial complex: How the American government is conscripting businesses and individuals in the construction of a surveillance society. New York. Retrieved November 8, 2008, from http://www.aclu.org/FilesPDFs/surveillance_report.pdf

American Civil Liberties Union (2006, January 31). Eavesdropping 2010: What can the NSA do? [Web page] Retrieved January 2, 2013, from http://www.aclu.org/files/pdfs/eavesdropping101.pdf

Bardin, J. (2012, August 16). Giving aid and comfort. *Infosec island* [Web page]. Retrieved from http://www.infosecisland.com/blogview/22211-Giving-Aid-and-Comfort-to-the-Enemy.html

Benitez, J. (2012, April 11). Pentagon expanding international partnership to address ‘global cyber arms race. *ACUS website*. Retrieved from http://www.acus.org/natosource/pentagon-expanding-international-partnerships-address-global-cyber-arms-race

Bijl, J. (2012, April 12). Critical analysis of Microsoft operation B71. *Fox IT blog* [Web page]. Retrieved from http://blog.fox-it.com/2012/04/12/critical-analysis-of-microsoft-operation-b71/

Boscovich, R. D. (2012, March 25). Microsoft and financial services industry leaders target cybercriminal operations from Zeus botnets . *The official Microsoft blog* [Web page]. Retrieved from http://blogs.technet.com/b/microsoft_blog/archive/2012/03/25/microsoft-and-financial-services-industry-leaders-target-cybercriminal-operations-from-zeus-botnets.asp

Brito, J. & Watkins, T. (2011, April). Loving the cyber bomb? The dangers of threat inflation in cybersecurity policy. Retrieved November 2, 2012, from http://mercatus.org/publication/loving-cyber-bomb-dangers-threat-inflation-cybersecurity-policy

Bryden, A. & Caparini, M. (2006). Private actors and security governance. Münster: Lit Verlag.

Calabresi, M. (2010, December 2). WikiLeaks' war on secrecy: Truth's consequences. *Time magazine* [Web page]. Retrieved December 3, 2011, from http://www.time.com/time/magazine/article/0,9171,2034488,00.html

CeBIT 2012: Eugene Kaspersky Calls for International Cyber-security Organisation. (2012, March 9). *Bizcomm,* Retrieved March 15, 2012, from http://www.bizcommunity.com/Article/82/391/72039.html

Clark, G. & Sohn, L. B. (1958). *World peace through world law*. Harvard University Press.

Czosseck, C., Ottis, R., & Talihärm, A. (2011). Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security . In *Proceedings of the 10th european conference on information warfare and security at the Tallinn University of Technology Tallinn, Estonia 7-8 july 2011* (pp. 57-64). Retrieved September 4, 2012, from http://www.ccdcoe.org/articles/2011/Czosseck_Ottis_Taliharm_Estonia_After_the_2007_Cyber_Attacks.PDF

Dafermos, G. (2012). Authority in peer production: The emergence of governance in the freebsd project. *Journal of Peer Production*, (1). Retrieved January 1, 2012, from http://peerproduction.net/issues/issue-1/peer-reviewed-papers/

Davis, J. (2007). Hackers take down the most wired country in europe. *Wired Magazine*, *15*(9), 15-09.

Deibert, R. (2010). Militarizing cyberspace - to preserve the open internet we must stop the cyber arms race. *Technology Review* . Retrieved January 10, 2012, from http://www.technologyreview.in/web/25901

Eilstrup-Sangiovanni, M. (2007, October). *Varieties of cooperation: Government networks in international security*. Florence: European University Institute, Robert Schuman Centre for Advanced Studies. EUI Working Papers RSCAS 2007/24. Retrieved April 20, 2009, from

http://cadmus.iue.it/dspace/handle/1814/7503

Estonian Defence League. (2010, December 20). Estonian defence league.. Retrieved December 21, 2010, from http://en.wikipedia.org/wiki/Estonian_Defense_League

Estonian Ministry of Defence (2011, January 20). Government formed cyber defence unit of the defence league. *Website of ministry of defence* [Web page]. Retrieved January 25, 2011, from http://www.mod.gov.ee/en/government-formed-cyber-defence-unit-of-the-defence-league

FBI New York Field Office (2011, November 9). Manhattan U.S. Attorney charges seven individuals for engineering sophisticated Internet fraud scheme that infected millions of computers worldwide and manipulated Internet advertising business . Retrieved May 13, 2012, from http://www.fbi.gov/newyork/press-releases/2011/manhattan-u.s.-attorney-charges-seven-individuals-for-engineering-sophisticated-internet-fraud-scheme-that-infected-millions-of-computers-worldwide-and-manipulated-internet-advertising-business

Ferguson, R. (2012, March 27). Don't be dumb, keep schtumm! . *CounterMeasures - trend micro blog* [Web page]. Retrieved January 10, 2013, from http://countermeasures.trendmicro.eu/dont-be-dumb-keep-schtumm/

Forward-Looking Threat Research Team (2012). *Operation Ghost Click - the Rove Digital takedown* (Trend Micro Incorporated Research Paper). Retrieved September 19, 2012, from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the_rove_digital_takedown.pdf

Friedman, T. (1998). Techno-Nothings. *New York Times,* p. 13. Retrieved October 7, 2003, from http://www.gsu.edu/~poljsd/3400/3400readings/techno-nothings.html

Gomez, W. (Transcript author). (2012). Building a secure cyber future: Attacks on Estonia, five years on. (Transcript of the ACUS workshop on May 23, 20012, Washington D.C). The Atlantic Council of the United States. Retrieved August 24, 2012, from http://www.acus.org/print/70435

Gorman, S. & Barnes, J. E. (2011, May 31). Cyber combat can count as act of war. *Wallstreet Journal,* Retrieved from http://professional.wsj.com/article/SB10001424052702304563104576355623135782718.html

Gruszczak, A. (2008). Networked security governance: Reflections on the EU's counterterrorism approach. *Journal of Global Change and Governance*, *1*(3).

Healey, J. (2012, January). Beyond attribution: Seeking national responsibility for cyber attacks. *Atlantic council issuebrief*. Retrieved April 3, 2012, from http://www.acus.org/publication/beyond-attribution-seeking-national-responsibility-cyberspace

Jackson Higgins, K. (2012, July 26). Apple makes black hat debut. *Dark reading* [Web page]. Retrieved July 30, 2012, from http://www.darkreading.com/mobile-security/167901113/security/vulnerabilities/240004456/apple-makes-black-hat-debut.html

Jackson Higgins, K. (2012, June 6). Siemens enhances security in post-stuxnet SCADA world. *Dark reading* [Web page]. Retrieved June 20, 2012, from

http://www.darkreading.com/advanced-threats/167901091/security/vulnerabilities/240001644/siemens-enhances-security-in-post-stuxnet-scada-world.html

Jung (2009). The "networked security" concept – stocktaking and perspectives. *European Security and Defence*, (1), 7-12. Retrieved June 28, 2009, from http://www.europeansecurityanddefence.info/Ausgaben/2009/01_2009/01_Jung/ESD_0109_Jung.pdf

Kahler, M. (2009). Networked politics: Agency, power, and governance. In M. Kahler (Ed.), *Networked politics: Agency, power, and governance* (pp. 1-21) [Web]. Cornell: Cornell University Press.

Kempa, M., Carrier, R., Wood, J., & Shearing, C. (1999). Reflections of the evolving concept of 'private policing'. *European Journal on Criminal Policy and Research*, *7*(2), 197-223. doi:10.1023/A:1008705411061

Klimburg, A. (2011). Mobilising cyber power. *Survival*, *53*(1), 41-60. doi:10.1080/00396338.2011.555595

Kolakowski, N. (2010, March 3). Spain, IT security companies sting Mariposa botnet. *eWeek*. Retrieved August 2, 2012, from http://www.eweek.com/c/a/Security/Spain-IT-Security-Companies-Sting- Mariposa-Botnet-390027

Korps Landelijke Politiediensten (2011, February 16). *Evaluatie tolling - lnnovatieve hoogtepunten en processuele lessen*. Retrieved October 7, 2012, from https://rejo.zenger.nl/files/0000034/20110216-evaluatie-tolling.pdf

Krahmann, E. (2005). Security governance and networks: New theoretical perspectives in transatlantic security. *Cambridge Review of International Affairs*, *18*(1), 15-30. doi:10.1080/09557570500059514

Krahmann, E. (2010). *States, citizens and the privatization of security*. Cambridge, UK, New York: Cambridge University Press.

Krebs, B. (2012, April 16). Microsoft responds to critics over botnet bruhaha. *KrebsOnSecurity* [Web page]. Retrieved January 10, 2013, from http://krebsonsecurity.com/2012/04/microsoft-responds-to-critics-over-botnet-bruhaha/

Kuerbis, B. (2011). Securing Critical Internet Resources: Influencing Internet Governance through Social Networks and Delegation (Doctoral Thesis). Syracuse University, iSchool - Information Science and Technology.

Kuerbis, B. & Mueller, M. (2011). Negotiating a new governance hierarchy: An analysis of the conflicting incentives to secure Internet routing. *Communications and Strategies*, (81), 125-142.

Lake, D. A. (2009). Hobbesian hierarchy: The political economy of political organization. *Annual Review of Political Science*, *12*, 263-283. doi:10.1146/annurev.polisci.12.041707.193640

Lamo, A. (2013, January 3). Bradley Manning and me: Why I cannot regret turning in the

WikiLeaks suspect. *The guardian* [Web page]. Retrieved January 11, 2013, from http://www.guardian.co.uk/commentisfree/2013/jan/03/bradley-manning-wikileaks-suspect-adrian-lamo

Landler, M. & Markoff, J. (2007). In Estonia, what may be the first war in cyberspace. *International Herald Tribune*. Retrieved November 4, 2010, from http://www.iht.com/articles/2007/05/28/business/cyberwar.php

Larraz, T. (2010, March 3). Spanish "botnet" potent enough to attack country: Police. *Reuters*. Retrieved January 16, 2013, from http://www.reuters.com/article/2010/03/03/us-crime-hackers-idUSTRE6214ST20100303

Lawson, S. & Gehl, R. W. (2011, May). Convergence security: Cyber-Surveillance and the biopolitical production of security. (Paper prepared for Workshop on Cyber-Surveillance in Everyday Life: An International Workshop, May 12-15, 2011, University of Toronto).

Lennon, M. (2012, March 26). Microsoft leads sting operation to disrupt Zeus botnets. *SecurityWeek*. Retrieved May 13, 2012, from http://www.securityweek.com/microsoft-and-partners-disrupt-zeus-botnets-sting-operation

Leyden, J. (2010, March 3). How FBI, police busted massive botnet. *The register*. Retrieved January 10, 2013, from http://www.theregister.co.uk/2010/03/03/mariposa_botnet_bust_analysis/

Macdonald, D. & Manky, D. (2010, February). Zeus: God of DIY botnets. *Fortiguard blog* [Web page]. Retrieved January 10, 2013, from http://www.fortiguard.com/analysis/zeusanalysis.html

Mandelbaum, M. (2006). The case for Goliath: How America acts as the world's government in the twenty-first century. PublicAffairs.

Markle Foundation - Task Force on National Security in the Information Age (2002, October). Protecting America's freedom in the information age. A report of the markle foundation task force.

McConnell, M. (2010, February 28). Mike McConnell on how to win the cyber-war we're losing. *Washington Post,* Retrieved November 4, 2012, from http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html

Minkwitz, O. & Schöfbänker, G. (2000). Information warfare: Die Rüstungskontrolle steht vor neuen Herausforderungen. Für eine Informationskriegsordnung: Frühzeitige Rüstungskontrolle statt Rüstungswettlauf. Berlin: Forschungsgruppe Informationsgesellschaft und Sicherheitspolitik. FoG:IS Arbeitspapier 2.

Mueller, M., Schmidt, A., & Kuerbis, B. (2013). Internet security and networked governance in international relations. *International Studies Review*.

de Natris, W. (2012, May 22). Public private cooperaration: The Zeus take down example. *Personal blog* [Web page]. Retrieved January 10, 2013, from http://woutdenatris.wordpress.com/2012/05/22/public-private-cooperaration-the-zeus-take-down-example

Nye, J. S. (1990). Bound to lead: The changing nature of American power. Basic Books.

Nye, J. S. (2011a). Nuclear lessons for cyber security? *Strategic Studies Quarterly*, *5*(4), 18-38.

Nye, J. S. (2011b). Power and foreign policy. *Journal of Political Power*, *4*(1), 9-24. doi:10.1080/2158379X.2011.555960

Openbaar Ministerie (2010, October 25). Nationale recherche haalt berucht botnet neer. Retrieved January 10, 2013, from http://www.om.nl/actueel/nieuws-_en/@154337/nationale_recherche_0

Ottis, R. (2010, November 19). Cyber security conference in Georgia. *Personal blog - conflicts in cyberspace* [Web page]. Retrieved January 11, 2013, from http://conflictsincyberspace.blogspot.com/2010/11/cyber-security-conference-in-georgia.html

Pear, R. (2012, April 26). House votes to approve disputed hacking bill. *New York Times,* Retrieved January 11, 2013, from http://www.nytimes.com/2012/04/27/us/politics/house-defies-veto-threat-on-hacking-bill. html

Porter, M. A., Onnela, J. P., & Mucha, P. J. (2009). Communities in networks. *Notices of the AMS*, *56*(9), 1082-1097.

Poulsen, K. (2007, August 22). 'Cyberwar' and Estonia's panic attack. *Wired, threat level*. Retrieved November 10, 2010, from http://www.wired.com/threatlevel/2007/08/cyber-war-and-e/

Raustiala, K. (2002). The architecture of international cooperation: Transgovernmental networks and the future of international law. *Virginia Journal of International Law*, *43*. Retrieved July 4, 2012, from http://ssrn.com/abstract_id=333381

Schmidt, A. (2012). At the boundaries of peer production: The organization of Internet security production in the cases of Estonia 2007 and Conficker. *Telecommunications Policy*, *36*(6), 451-461. doi:10.1016/j.telpol.2012.02.001

Schmidt, A. (2013). The Estonian cyberattacks. In J. Healey (Ed.), *The fierce domain – conflicts in cyberspace 1986-2012*. Washington, D.C.: Atlantic Council.

Schwartz, M. J. (2010, October 27). Bredolab botnet busted. *InformationWeek*. Retrieved May 13, 2012, from http://www.informationweek.com/story/showArticle.jhtml?articleID=228000096

Shachtman, N. (2011, June). *Pirates of the ISPs: Tactics for turning online crooks into international pariahs*. Washington, D.C .: Brookings. Retrieved March 10, 2012, from http://www.brookings.edu/papers/2011/0725_cybersecurity_shachtman.aspx

Shachtman, N. (2012, July). Russia's top cyber sleuth foils US spies, helps Kremlin pals. *Wired*. Retrieved January 11, 2013, from http://www.wired.com/dangerroom/2012/07/ff_kaspersky/all/

Sinha, P., Boukhtouta, A., Belarde, V. H., & Debbabi, M. (2010). Insights from the analysis of the Mariposa botnet. In CRiSIS 2010, fifth international conference on risks and security of Internet and systems, Montreal, Canada, October 10-13, 2010 (pp. 1-9).

doi:10.1109/CRISIS.2010.5764915

Slaughter, A. M. (1997). The real new world order. *Foreign Affairs*, *76*(5), 183-197.

Slaughter, A. M. (2004). *A new world order*. Princeton, NJ: Princeton University Press.

Slaughter, A. M. (2009). America's edge-power in the networked century. *Foreign Affairs*, *88*(1), 94-113.

Sully, M. & Thompson, M. (2010, February). *The deconstruction of the Mariposa botnet*. Defence Intelligence. Retrieved September 16, 2012, from http://defintel.com/docs/Mariposa_White_Paper.pdf

Tabatabaie, S., van Eeten, M., & Asghari, H. (2012). Transgovernmental networks in cybersecurity: A quantitative analysis of the London Action Plan against spam. Paper presented at the 2012 Annual Convention of the International Studies Association.

van Eeten, M. (2010, November 1). Dutch police inflates Bredolab botnet success by factor of ten, and then some. *Internet governance project*. Retrieved November 2, 2010, from http://www.internetgovernance.org/2010/11/01/dutch-police-inflates-bredolab-botnet-success-by-factor-of-ten-and-then-some

von Eitzen, C. (2011, November 10). Operation Ghost Click: FBI busts DNSChanger botnet. *The H Security*. Retrieved May 13, 2012, from http://www.h-online.com/security/news/item/Operation-Ghost-Click-FBI-busts-DNSChanger-botnet-1376746.html

Weber, S. (2004). *The success of open source*. Cambridge, MA: Harvard University Press.

Wong, W. & Lake, D. (2009). The politics of networks: Interests, power, and human rights norms. In *Networked politics: Agency, power, and governance*. Ithaca, NY: Cornell University Press.