Freedom, Control, Security – Current and Future Implications for Internet Governance

Martin Hans Knahl

Faculty of Business Information Systems, University of Applied Sciences Furtwangen, Robert-Gerwig-Platz 1, 78120 Furtwangen / Germany

knahl@hs-furtwangen.de

Geoff Cox

Center for Digital Urban Living, Department of Information & Media Studies, Aarhus University, Helsingforsgade 14, DK-8200 Aarhus N / Denmark

imvgc@hum.au.dk

**Abstract**

Internet Governance is concerned with the organisation, control, and strategic development of the Internet. It is a relevant and widely debated topic lacking universal consensus. Furthermore, from the operational perspective, administrative control and technical operation of the Internet are crucially relevant issues for the global dissemination of information, online virtual communities and the global economy. Thus political and technological aspects and considerations are interwoven and cannot be separated. Key Internet operation and maintenance organisations such as the Internet Corporation for Assigned Names and Numbers (ICANN) are currently in the process of formulating the scope and agenda of future Internet governance with significant implications for online services. Such developments are thereby having a major impact and are strongly present in the operation of the Internet with further implications regarding Internet security and control aspects inside Internet groups and communities. Governance and security are issues necessitated on protection from perceived chaos, real or symbolic violence or even terrorism, but who governs and secures the Internet against such threats? Indeed who will protect us from security? These issues are discussed at different scales and the article uses the example of Botnets to demonstrate how control is distributed both horizontally and vertically in keeping with contemporary forms of governance and security, reflected in the technical infrastructures of the Internet itself.

INTRODUCTION

*“Then there is electricity — the demon, the angel, the mighty physical power, the all-pervading intelligence... Is that a humbug too? Is it a fact… that, by means of electricity, the world of matter has become a great nerve, vibrating thousands of miles in a breathless point of time? Rather, the round globe is a vast head, a brain instinct with intelligence! Or shall we say it is itself a thought, nothing but thought, and no longer the substance which we deemed it!”*

*“If you mean the telegraph… it is an excellent thing — that is, of course, if the speculators in cotton and politics don’t get possession of it. A great thing… particularly as regards the detection of bank robbers and murderers.”*

(Hawthorne, 1851)

The thoughts of the writer Nathaniel Hawthorne were inspired by the development of electricity and the telegraph in the mid 19th century. Much as Jules Verne envisioned extensive journeys and moon landings, Hawthorne tried to foresee the contradictory possibilities of electronic communication. Hawthorne speculates that global connectivity may lead to new horizons, a claim that has been repeated with regards to the Internet by more contemporary commentators (Lessig, 2006; Mitchell, 1996). Given the widespread use and alleged pervasiveness, the questions of how to develop, operate and control the Internet involves the controversial and complex issue of governance.

*Figure 1: Internet Governance Regulators*

The term *governance* derives from the Greek verb κυβερνάω (*kubernáo*) meaning *to steer* (and thus also making reference to cybernetics) and generally politics provides the means by which the governance process is operated (Wikipedia, 2010).Conceiving of Internet governance in this way, one can encounter the process in States and State organisations, profit and non-profit corporations, NGOs and other associations (e.g. social networks, project-teams) engaged in the general operation, management and control of Internet-related activities (Marsden, 2008). A number of regulators impact upon the process and define the role and limitation of Internet Governance; for instance compare the issues relating to Architecture, Market, Norms and Regulation in figure 1 (Lessig, 2006: 123). These different aspects clearly impact upon governance and confirm it as a political issue, for example in the social costs of the Internet. Solum further identifies cybersquatting as a prime example of social costs: the “registration of a domain name that infringes a trademark for the sole purpose of extracting a payment for transfer of the domain name” (Bygrave, 2009). This lies in contrast to the Coase-Theorem (associated with the economist Ronald Coase) that states that the assignment of entitlements does not affect the efficiency of outcomes (i.e. that the distributional effect does not result in economic inefficiency), so that negotiations between cybersquatters and trademark owners generate positive transaction costs. Hence regulations (e.g. in the form of national and international trade laws, Domain Name policies) can facilitate and steer this process as part of Internet governance.

Trust in the governance process of the Internet and further between users is a key factor for users in any online community (such as those derived from social networks or those using online transaction services). Liu et. al. (2008) address the problem of predicting whether users trust each other and propose a classification approach to address what they refer to as the trust prediction problem. They develop a taxonomy to obtain an extensive set of key features derived from user attributes and user interactions in an online community and demonstrate that trust among users can be effectively predicted using pre-trained classifiers. Thus the aim is to recognise security requirements and to ultimately design and implement trust into any online experience. In a widely cited paper, Ben Shneiderman proposed two key principles associated with this: “*Invite participation by ensuring trust"* and *“Accelerate action by clarifying responsibility“, together with guidelines such as “disclose patterns of past performance“*, *“get certifications from third parties“*, *“clarify each participant’s responsibilities“* or *“*provide clear guarantees with compensation“(Shneiderman, 2000). Governance in this sense is tied to the idea of encouraging users to largely govern themselves through their active participation (Foucault, 2010), and this is the case with Internet developments in general.

The Development Context

Saltzer, Reed and Clark (1984) define the End-to-End principle of the Internet. It manifests that the inherent implementation and features of the Internet services themselves are placed on the edge of the network rather than within the core of the network (Saltzer, 1984). The End-to-End principle has been the foundation of the ARPANET and the Internet. It still provides the fundamental, if somewhat compromised, characteristic of all communication services (Saltzer, 1984; Bygrave 2008; Lessig, 2006) and has proved crucial for the development of new services such as Messaging or E-Mail. Soon after the creation of the ARPANET, the service of sending messages from individual to individual on a one-to-one and one-to-many basis became widely used. Licklider, one of the early system administrators of the early ARPANET described the use of the messaging service:

*“It soon became obvious that the ARPANET was becoming a human-communication medium with very important advantages over normal U.S.* *mail and over telephone calls. One of the advantages of the message systems* *over letter mail was that, in an ARPANET message, one could write tersely* *and type imperfectly, even to an older person in a superior position and even* *to a person one did not know very well, and the recipient took no offense.* *The formality and perfection that most people expect in a typed letter did not* *become associated with network messages, probably because the network* *was so much faster, so much more like the telephone.” (Licklider & Vezza, 1978)*

Other forms of communication, associated with what Howard Rheingold coined “virtual communities” in 1994 (Rheingold, 1994) would become referred to as weblogs or blogs, further facilitating user-oriented content generation:

*“The liberating news about virtual communities is that you don’t have to be a professional writer, artist, or television journalist in order to express yourself to others. Everyone can be a publisher or a broadcaster now. Many-to-many communications media have proved to be popular and democratic” (Rheingold, 2002: 121)*

In the meantime, E-Mail and ongoing service innovations such as the World Wide Web (WWW) have become widely used and essential tools of personal and business interaction. Its relative impact is comparable to the introduction of regular mail service and trade when introduced centuries ago albeit at a very short period of time. Mitchell argues that just as railroads have been a major influence on settlement patterns and economics of the 19th century, and as automobiles have further influenced settlement, commerce and recreation in the 20th century, computer networks will influence our daily life to a large extent in the 21st century (Mitchell, 2000). The relative openness, fastness and cheapness of communication services have wide ranging political and governance implications that have only recently begun to be explored (Hart, 2008). One challenge for Internet governance is how to preserve the overall positive effects of the lower cost of transactions and the pervasiveness of global communications, whilst making sure that values such as personal privacy, market transparency and even national security are also protected. E-mail for example is the primary vehicle for distributing spam, viruses, worms, phishing expeditions and denial of service attacks.

Furthermore, Cloud Computing, the trend of placing services and data onto the Internet itself (and not on the users’ hard disc) has the potential to turn the Internet into an all encompassing utility, comparable to the electric utilities that changed how businesses operated and brought the modern world into existence (Carr, 2009). A tension between freedom and control is further invoked in such developments as communications technologies and new forms of governance converge.

In his book "City of Bits", Mitchell reflects upon this tension inherent to the architecture of the Internet and the communities it serves:

*“Architecture, laws, and customs maintain and represent whatever balance has been struck. As we construct and inhabit cyberspace communities, we will have to make and maintain similar bargains - though they will be embodied in software structures and electronic access controls rather than in architectural arrangements… since electronic data collection and digital collation techniques are so much more powerful than any that could be deployed in the past, they provide the means to create the ultimate Foucaultian dystopia."* (Mitchell, 2000)

That may be the case. Hart (2008) concludes that current research on “*Internet issues and governance forums tends to focus primarily on the domain name system and ICANN, including research on WSIS, even though many other crucial issues, and particularly those associated with e-commerce and trade in digital products in the WTO and the OECD are of equal importance.*” Hart (2008) further argues that *“North-South forums like … WSIS are important more as a proving ground for the idea of a ‘multi-stakeholder approach’ to global governance than for describing and explaining the most important emerging international regimes for ICTs*” and that “*the G8 and the OECD, are considerably more important overall for ICT regime creation and maintenance*”. So whilst it is clear that governance issues are important at the level of legislation and policy, it is also clear that network forms of organization actually prescribe control structures. The ability of networked communication technologies to allow interconnections indicates their ideological power, and despite appearances how scale-free networks contain hubs and hierarchies. Barabási (2002) indicates how scale-free networks like the Internet can be seen to offer “directness”.

Although the Internet is largely non-hierarchical in structure, conforming to the way TCP/IP connects one machine to others, it is also subject to the DNS (domain name system) information stored in decentralised databases, organised in hierarchical, inverted tree-structures. For example, in the current model the Internet's address structure (DNS), which enables communication between the world’s computers, is managed by the California-based, not-for-profit Internet Corporation for Assigned Names and Numbers (ICANN) under contract to the US department of commerce (Wray 2005). In question is the centralisation of control and whether other countries should be allowed more control over their Internet domains. Barabási (2002) also reveals that the Internet is organized into four continents so is hardly the metaphor of global community it purports to be. That ICANN are currently in the process of formulating the scope and agenda of future Internet governance holds significant implications for online communities. Clearly more detail is required to understand how networks operate both technically and politically.

One of the key challenges for social trust in Virtual Communities is estimating how much users will trust each other (Globeck, 2008). Given the billions of users on the Web and hundreds of online social networks with more than a billion accounts among them, it is thus rather unlikely that any two users will know one another in the classical sense. This leads to challenges with regards to identity and authenticity. Privacy Enhanced Mail (PEM), is an early IETF proposal specified in RFC 1421 in February 1993 to provide secure email communication using public key cryptography. Given its dependency on prior deployment of a hierarchical public key infrastructure (PKI) with a single root, it lacked market acceptance and was not widely deployed or used. Deployment of a PKI proved difficult due to high operational costs and legal implications (i.e. legal liability of the root and 'policy' Certificate Authorities). From a governance point of view, such an approach is controversial given the inherent imposition of a central authority. Thus opposition to this approach became widespread and alternative approaches were proposed, notably Phil Zimmermann’s Web of Trust as the PKI infrastructure for Pretty Good Privacy (PGP). Web of trust is a concept used in PGP and other OpenPGP compatible systems to authenticate the binding between a user on one hand and a public key on the other hand. As with Virtual Communities, there are many independent webs of trust, and any user can belong to multiple webs through their identity certificate. Pretty Good Privacy (PGP) provides data encryption and decryption to ensure cryptographic privacy and authentication for data communication thus providing a basis service for Virtual Communities. PGP is often used for signing, encrypting and decrypting e-mails to increase the security of e-mail communications.

Security Implications: The Case of Botnets

The global increase of Internet connectivity (e.g. based on “always-on” broadband connections) undoubtedly brings tremendous economic and social opportunities. However, software developers and *malware* authors have also discovered great potential facilitated through vulnerable Internet service, operating systems and inept Internet users (Grizzard, 2007). As security threats increase typical users remain ignorant of what an expert might call "common-sense” approaches to avoid being compromised (or to keep systems “uninfected”). These are facilitated through virus propagation, spam, click fraud, phishing, and activities have boomed through collections of software robots, or bots, that run autonomously– collectively referred to as *Botnet*s . Botnets can refer to a network of computers using distributed computing software but are typically associated with malicious software. A Botnet usually constitutes a collection of compromised computers (sometimes also referred to as Zombie computers) running software usually installed via worms, Trojan horses or backdoors under a common command-and-control infrastructure. The majority of these computers are running Microsoft Windows operating systems, but other operating systems can be affected. Numerous Botnets have been found on the Internet, and examples include a Botnet discovered by the Dutch police with a reported number of 1.5 million nodes (Keitzer, 2005) and a 10,000-node Botnet discovered and apparently dismantled by the Norwegian ISP Telenor (Leyden, 2004). To further counteract Botnets international coordinated efforts to discover and remove Botnets have also been initiated (Leyden, 2005)*.* It is believed that the majority of Botnets today are used to distribute spam. In this way a spammer can use captured systems to transmit millions of messages simultaneously. As these messages are sent through the email systems of “ordinary” users may further increases resilience with regards to spam filters. The program installed by a Botnet may further violate a system’s hard disc and monitor its user's keystrokes to gather private data.

Botnets have been identified as one of the key threats to network security, especially the peer-to-peer (P2P) based Botnets. One way of countering botnets is by target-attacking the weaknesses of high degree nodes or edges of the botnets (Li et al, 2010). Security experts need to know the features of the topology of botnets. Inspired by the method of complex network, Li et al (2010) propose a growing model of botnets that focuses on the network metrics of Botnets.

Botnets provide us with a good example to reveal the inherent structures and topology of the Internet and how freedom and control – as in the case of Virtual Communities - are negotiated, if not compromised. In cases of security violation, it can be demonstrated how networks are a manifestation of ideology. This is what Galloway and Thacker describe, in “The Exploit” (taking their title from a term used by crackers to take advantage of vulnerabilities in networks), as the new ”network-network symmetry” of power in which control is distributed relatively autonomously in horizontal organisational locales and at the same time into rigid vertical hierarchies or directed commands (Galloway & Thacker, 2007). Their description is a socio-technical truism of course, and one that supports their claim that networks and sovereignty are not incompatible. This is precisely what software developers and malware authors have discovered, as they *exploit* vulnerable operating systems, Internet service and security software. Tactics are propagated through various means such as Botnets.

In response the area of software security is a booming industry, and a number of security-industry recommendations and standards have been developed. An understanding of the characteristics and nature of known vulnerabilities has also been organised into taxonomies, providing a framework for the examination of known and potential future vulnerabilities. Early work on security related taxonomies has been carried out since the 1970s with varying degree of effectiveness. These can provide a framework for the examination of known and potential future vulnerabilities. Igure et al (2008) suggest the following properties for an efficient taxonomy of attacks and vulnerabilities in Computer Systems:

• Application- or system-specific taxonomy

• Taxonomy must be layered or hierarchical

• First level of classification — attack impact

• Second level of classification — system-specific attack

• Third level of classification — system components (attack targets)

• Fourth level of classification — system features (source of vulnerability)

• Classes need not be mutually exclusive

Rogue software is usually installed via worms, Trojan horses or backdoors under a common command-and-control infrastructure. A program installed by a Botnet can violate a system’s hard disc and monitor its user's keystrokes to gather private data from services (such as sensitive financial information, including credit card numbers and passwords for bank accounts). The retrieved data is then distributed over the Internet to its ‘master’.

A number of major Botnet source codebases such as Agobot, SDBot, SpyBot have been identified and discussed in literature (Cook, 2005; Harford, 2006). Harford (2006) suggests that Agobot, also commonly referred to as Phatbot, is based on the most sophisticated Botnet source code (e.g. when compared to SDBot and SpyBot) and consists of around 20.000 C/C++ lines of code.



*Table 1: Agobot commands, comp. (Harford, 2006)*

A typical Botnet implementation contains of numerous components such as an Internet Relay Chat (IRC) command and control mechanism and services to compromise security (e.g. to collect Paypal passwords or search registry entries). Thus the Botnet command language is derived from standard IRC as defined by the Internet Engineering Task Force (Kalt, 2000) and includes directives to request a bot to perform specific functions such as bot.open to open a specific file on a compromised host. Thus close monitoring of IRC related traffic can facilitate the detection of Botnets through the identification of anomalies. Propagation mechanisms enable the Botnet to scan for and detect new systems for the Botnet. One mechanism is to take advantage of the IP addressing structure that is based on network, subnet and host IDs to implement the scanning of entire IP address ranges. The exploitation and attack mechanisms are generally attempted in combination with propagation and scanning and provide various means to attack a system (e.g. Agobot provides a brute-force password scanner for SQL servers and different types of generic denial of service attacks such as HTTP floods in the DDoS module).

Botnets can undoubtedly cause severe disruption on targeted sites. A Botnet can control a set of ‘hijacked’ systems to target systems (e.g. a community, commercial or government website) with information requests in a distributed denial of service (DDoS) attack. In the extreme, a system that is unable to handle excessive crashes, sometimes brings down an entire data centre with it. One prominent example is Six Apart, an American blog publisher that became involved in a Distributed Denial of Service (DDOS) attack of a Botnet in May 2006. Within the course of minutes, the company's servers had become unavailable and the blogs of 10 million customers disappeared. Six Apart eventually discovered that the attack was not aimed at itself but rather at one of its customers, an Israeli firm named Blue Security, which had caused ignominy by offering a spam-counter attack service (Berinato 2006). However the Botnet assault continued for weeks, damaging many other companies and sites. Eventually Blue Security surrendered and went out of business, expressing their reluctance to take part in an ever-escalating battle.

There are countless other cases that illustrate insecurity issues surrounding Botnets and the ways in which vulnerability in the system is exploited in communities. With the popularity of filesharing and the high volumes of computers connected to Peer-to-Peer (P2P) networks, systems have also become increasingly open to attack. The Trojan.Peacomm is an example of a Trojan Horse that provides the basis for building a P2P Botnet (Grizzard, 2007). The threat typically arrives in an email with a subject (e.g. ‘U.S. Secretary of State Condoleezza Rice has kicked German Chancellor Angela Merkel’), and attachments (e.g. ‘Full Story.exe’) and an empty body. The executable is a Trojan Horse which modifies a system’s services.exe process and adds hidden threads. The ‘infected’ system subsequently attempts to establish P2P communication via UDP using a set of given IP addresses to obtain additional malicious files. Using a firewall with egress filtering, it can be detected that the services.exe process attempts to connect to a remote address via a UDP port. Subsequently the system will receive additional IP addresses, in essence building up a distributed network. To facilitate the process, the Trojan further maintains a list of unsuitable peers. The strategy of using peer-to-peer communication spreads the load and further improves the robustness of the Botnet, particularly when compared to the traditional approach of using centralised command & control servers.

It is fraught with danger to precisely estimate the size of the problem and this in itself generates insecurities of another type. Some computer security experts believe that at least 10% of home PCs have been recruited into Botnets (Carr, 2007). Other analysts, including Vint Cerf (one of the inventors of the Internet and now a top Google executive one of the pioneers of the Internet) was quoted at the World Economic Forum in February 2007 that Botnets have become "pandemic" and that up to one quarter of all systems connected to the Internet may become part of a Botnet (Carr, 2007; Weber, 2007). It would appear that the issue of security is reducible to the challenge of managing the inherent insecurities of networked relations. The many examples serve to demonstrate how control is distributed both horizontally and vertically and that online communities provide the territory for this activity. The ability of networked communications technologies to allow interconnections and participation indicates their power, and despite surface appearances how scale-free networks demonstrate directedness.

It can be concluded that botnet attacks impose serious threats to the modern Internet and Virtual Communities. Given that money is a determining force driving the growth in botnet attacks, Lie e. Al. (2009) propose an economic approach to take away the financial incentives by introducing the uncertainty level to make the optimal botnet size infeasible for the botnet operators. Thus as the chance of uncertainty increases, both botnet masters’ and attackers’ profits can fall dramatically.

Conclusion: The case for A BETTER UNDErstanDING OF SECURITY AND NETWORKS

The loosely coupled, hierarchical and ultimately insecure networks of the internet, with their ever growing numbers of users and capacity, provide a challenging environment to ensure common policies and behaviour based on suggested principles. Rheingold (2000) and other authors agree that Virtual Communities that embed many of the nuances of public conferencing, private communication or hybrid entities will require changes in these principles. However, Rheingold (2000) further states that the identification of these issues provides a platform to focus societal debate about values, risks, and liberties. Thus if substantial financial benefits or control can be derived through “Net-snooping”, and the inherent architectural principles of the Internet make it difficult to protect Virtual Communities on one side and to track perpetrators on the other, no regulation or law will ever be able to adequately protect Virtual Communities and individual users.

The tension between freedom and control is inherent to the Internet and the communities it serves reflecting its contradictory development. Lessig argues that the initial variant of the Internet rendered difficult for politics to control Internet usage and developments whilst “software was the product of hackers and individuals outside of any institution of effective control” (e.g. Universities or research institutes) (Lessig, 2006: 72). However, he further concludes that “as code has become the product of companies, the power of [politics] has increased” given the fact that “when commerce writes code, then code can be controlled, because commercial entities can be controlled” (Lessig, 2006: 72).

The security industry’s nested interests of creating awareness or even fear regarding perceived insecurity is impacting upon the ability of users and online communities to assess the latest developments in security. This creates a power differential, where a number of companies, together with the media, exercise immense control over the notion of security (Cox & Knahl, 2009). Thus, in the style of a self-fulfilling prophecy, the industry intensifies the dependency of the users to get the latest security intensified by feelings of insecurity. According to different market surveys the size of the IT security market is experiencing rapid growth (Thomson, 2008). Given that estimates of the size of the security market will vary depending on the source, the included elements of when, how and for whom the data was collected means the actual size is difficult to establish. According to figures from Gartner, sales of enterprise security products rose by nearly 20 per cent in 2007 and were worth $10.4bn. According to Gartner, Symantec is market leader (26%) followed by McAfee (11%) and the strongest growth is in the area of Email security (45%); from a geographical perspective, Latin America is the fastest growing region for Enterprise Security Products (over 40% sales growth) and North America (47.5%) and Western Europe (31.7%) have the biggest market share (Thomson 2008). Ruggero Contu from Gartner has been quoted that “compliance, data leakage and privacy issues, along with the need to tackle the fast evolving and sophisticated threat environment, are among the major drivers fuelling the growth of spending on security” (Thomson, 2008).

Furthermore Post and Kagan (2007) raise the pressing question whether IT security controls are a burden or benefit. According to the results of their study *“34% of the respondents perceived interference or delays caused by the computer security systems as a consequence of their current business environment… general employees perceive that increases (more onerous measures) in security policies and practices result in greater interference(s) with their job responsibilities.”* They suggest that users should be part of creating a security policy and suggest the testing of security restrictions on users to minimize task interference. In this sense online communities might begin to take more control over their security needs and thus perhaps develop less paranoid responses based on a better understanding of the Internet’s vulnerabilities.

The point is that the issue of security demonstrates some of the core principles that relate to governance more generally under neoliberal conditions. To add detail here, many commentators turn to Foucault's lectures on governmentality delivered between 1982-3 (Foucault, 2010). Foucault draws out a distinction between early liberalism and contemporary neoliberalism. Neoliberalism replaces the regulatory function of the state to the market with the market itself, and emphasizes the human subject in different terms reacting to the market rather than the limits of government. The goal of government becomes the constitution of certain types of subjectivity in line with competition within, and reducible to, the logic of free markets. Like the scale-free network, a certain exercise of power is demonstrated.

What we wish to argue in this chapter is for better understanding of the networks that communities occupy in recognition of the need to rethink the way that power in managed within them. It is clear that networks reflect contemporary political dynamics and a technical awareness of this is also required to fully understand what is at stake. The architecture of the Internet is distributed and fragmented but nevertheless imagined in terms of its totality, which remains a fantasy. As the example of botnets aimed to demonstrate, further discussion is required on the relations between the human and inhuman elements that constitute the network. Networks involve shifts of scale such that action can no longer be attributed to individuals or communities but also to distributed coded actions that operate throughout it. Control and freedom and the feelings of security associated with both are distributed in keeping with the technical infrastructures of the Internet itself.

**REFERENCES**

Barabási, A-L. (2002). Linked: The New Science of Networks. Cambridge, Mass.: Perseus.

Barlow, John Perry (2000)*. The Debate Over Internet Governance: A Snapshot in the Year 2000*. Harvard. URL: http://cyber.law.harvard.edu/is99/governance/barlow.html [Last Accessed 2010-03-10]

Bygrave, Lee A. (2009)*. Internet governance: Infrastructure and institutions*. Oxford: Oxford Univ. Press. Online im Internet: URL: http://www.gbv.de/dms/spk/sbb/recht/toc/581075692.pdf

Carr, N. (2007). Botnets - a hidden menace that threaten the future of the Internet. The Guardian. 5 April 2007.

Carr, Nicholas G. (2008)*. The big switch: Rewiring the world, from Edison to Google.* 1. ed. New York: Norton. Online im Internet: URL: http://www.gbv.de/dms/bsz/toc/bsz27866685xinh.pdf

Cox, Geoff and Knahl, Martin (2009). Critique of Software Security. Book chapter in Wolfgang Sutzl (ed.): Creating Insecurity: Art and Culture in the Age of Security, New York: Autonomedia, pp. 27-43.

Foucault, M. (2010). The Government of Self and Others: Lectures at the College de France 1982-1983. Basingstoke: Palgrave Macmillan.

Galloway, A.R. & Thacker, E. (2007). The Exploit: A Theory of Networks. Minneapolis: University of Minnesota Press.

Globeck, Jennifer (2008). Weaving a web of trust. *Science*, 321:1640–1641.

Goth, G. (2007). Fast-Moving Zombies: Botnets Stay a Step Ahead of the Fixes. *IEEE Internet Computing.* Volume 11 (2): 7-9.

Grizzard, J. et al (2007). Peer-to-Peer Botnets: Overview and Case Study. HotBots '07 / 4th USENIX Symposium on Networked Systems Design & Implementation (NSDI '07). Cambridge (MA), 11-13 April 2007.

Hart, Jeffrey A. (2008). Global Internet Governance. *Conference of the International Public Affairs. Association of Indiana University, Bloomington, Indiana* 11 April 2008

Hawthorne, Nathaniel (1851)*. House of the Seven Gables*

Kalt, C. (2000). Internet Relay Chat: Architecture. Network Working Group / Internet Engineering Task Force Request for Comments: 2810. April 2000.

Keizer, G. (2005). Dutch Botnet Bigger Than Expected. *TechWeb Technology News*. Oktober 21, 2005.

Leyden, John (2004). Telenor takes down 'massive' Botnet. *Enterprise Security.* 9th September 2004.

Leyden, John (2005). ISPs urged to throttle spam zombies: International clean-up campaign. *The Register.* 24th May 2005.

Li, Zhen et al. (2009). Botnet Economics: Uncertainty Matters. In *Managing Information Risk and the Economics of Security*. Springer: 245-267.

Li, Xuefeng et al (2010). The growing model of Botnets. *2010 International Conference on* *Green Circuits and Systems (ICGCS):* 414-419.

Liu, H., Lim, E., Lauw, H. W., Le, M., Sun, A., Srivastava, J., and Kim, Y. (2008). Predicting trusts among users of online communities: an epinions case study. In *Proceedings of the 9th ACM Conference on Electronic Commerce* (Chicago, Il, USA, July 08 - 12, 2008). EC '08. ACM, New York, NY, 310-319.

Lessig, Lawrence (2006)*. Code: Version 2.0* (2nd ed.). New York: Basic Books

Lessig, Lawrence (2009). In Defense of Piracy. *The Wall Street Journal* 16. September. Online im Internet: URL: http://online.wsj.com/ar3cle/SB122367645363324303.html [Last Accessed 2009-12-12]

Licklider, J.C.R. and Vezza, Albert (1978). Applications of Information Networks. *Proceedings of the IEEE, 66*

Marsden, Christopher (2008). Beyond Europe: The Internet, Regulation, and Multistakeholder Governance—Representing the Consumer Interest? *Journal of Consumer Policy, Volume 31 (1).* Springer: 115-132.

Mitchell, William J. (2000)*. City of bits: Space, place, and the infobahn.* 7. print. Cambridge, Mass.: MIT Press

Post, G.V. and Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. Elsevier / Computers & Security. No. 26, 2007: 229-237.

Rheingold, Howard (2002). Smart Mobs: The Next Social Revolution. *Perseus. Cambridge, Mass.*

Rheingold, Howard (1994). *The Virtual Community: Homesteading on the Electronic Frontier.* *HarperPerennial New York*

Rheingold, Howard (2000). *The Virtual Community: Homesteading on the Electronic Frontier.* London: MIT Press.

Saltzer, Jerome H. and David P. (1984). End-to-end arguments in system design*. ACM Transactions on Computer Science*, 277–278.

Shneiderman, B. (2000). Designing trust into online experiences. *Communications of the ACM* 43, 12 (Dec. 2000).

Thomson, I. (2008). Enterprise security software market booms. vnunet.com. 18 June 2008. http://www.vnunet.com/vnunet/news/2219275/enterprise-software-market

Vinay M. Igure, Ronald D. Williams (2008). Taxonomies of Attacks and Vulnerabilities in Computer Systems. *IEEE Communications Surveys & Tutorials.* 1st Quarter 2008.

Weber, Tim (2007). Criminals 'may overwhelm the web'. BBC News website. 25 January 2007.

Wikipedia*. Governance*. URL: http://en.wikipedia.org/wiki/Governance [Last Accessed 2010-03-11]

Wray, R. (2005). EU says Internet could fall apart. The Guardian, 12 October 2005. http://technology.guardian.co.uk/news/story/0,16559,1589967,00.html

**KEY TERMS**

Internet, Governance, Security, Botnet, Networks, ICANN, IETF