# CONCEPTUALIZING INTERNET SECURITY GOVERNANCE

ANDREAS SCHMIDT, a.schmidt@tudelft.nl
Delft University of Technology, Faculty of Technology, Policy, and Management, Section ICT
P.O. Box 5015, 2600 GA Delft, Netherlands

Paper prepared for GIGANET conference, Sharm El-Sheik, Egypt, November 2009

Draft, version 04 (Nov 12, 2009); updated version will be available from the author upon request

Keywords: internet security, internet security governance, peer production

## 1. INTRODUCTION

Current internet security research seems to lack decent conceptualizations of internet security. At times, the idea of internet security seems to be simply based on anecdotical descriptions, partly driven by fear-mongering scenarios or framed by personal or organizational interests of authors or editors. Researching on internet security governance however precludes a clear conceptualization of the central term.

This paper seeks to conceptualize internet security governance by utilizing previous works in the fields of security studies, international relations, policing studies, social security policy analysis and computer science. What students of internet security governance can learn from non-internet security governance research is a) a more differentiated categorization of institutions and actors in security governance and, linked with that, b) the processualisation and segmentation of security provisioning. The internet is however regulated by more pluralized modes of governance. More philosophical discourses of security point at the narrowness of today's conceptualizations of internet security and suggest a broader, more political understanding of internet security.

In the first section, I will discuss the notion of security more generally. I will show that current conceptualizations of internet security lack depth and are loaded with ambiguities, thereby decreasing the analytical capabilities of the concept of internet security. The second section will analyze concepts of security governance and the way they are used in disciplines other than internet studies. And finally, this paper will break down security and its governance into their basic characteristics to be used for the analysis of internet security politics.

## 2. CHARACTERISTICS OF SECURITY

### 2.1. VAGUENESS OF 'INTERNET SECURITY'

Clarification of the meaning of a concept is a precondition for scholars, engineers, business persons and policy-makers to interpersonally and unambiguously communicate ideas, analysis and policy options. (Baldwin, 1997, pp. 5-6) An engineer talking about internet security might have very different things in mind than a strategic policy advisor: the ideas of a scholar can be meaningless to a politician if the latter has a binary understanding of security— there either is security or there is insecurity— and the former hasn't. Concepts of security aren't likely to merge into one universal concept of security. Nevertheless, researchers should be aware of possible differences in conceptualizations. For conceptualizations to become scientifically useful, a set of criteria helps to make them more appropriate: operationalizability, definitional connections to related terms, openness to any kind of empirical investigation, closeness to ordinary language. (Cf. discussion in Baldwin, 1997, p. 7)

In many studies, 'internet security' is often referred to as the absence or the proper handling of 'security problems' or 'security topics' like phishing, spam, viruses, and achieving technical resilience of the internet. (Anderson & Moore, 2007; Brown & Marsden, 2007) Threats to internet security are often described by terms like 'cyberattack', 'cybercrime', 'cyberterrorism', or 'cyberwar'. (Bendrath, 2003; Dunn Cavelty, 2007; Wilson, 2007) Others prefer 'cybersecurity' over 'internet security'. (International Telecommunications Union, 2005) While some link cyberwar to state actors by defining it as "deliberate disruption or corruption by one state of a system of interest to another state" (Libicki, 2009), others prefer a broader concept of cyberwar, which includes any type of actor. These examples indicate that the term 'internet security' suffers from the same problem that Myriam Dunn Cavelty has identified with regard to the term 'cyberterror' —it's "a very elusive and poorly defined concept"(Dunn Cavelty, 2007, p. 22); and these definitions don't meet the elaborated criteria set for conceptual explication in general.

What distinguishes internet security from other fields of security is the centrality of technology in this area of security. Computer scientists use a different concept of security than social scientists, one that appears to be less normatively enriched than in some political discourses where security is linked to questions of survival.

### 2.2. AVAILABILITY, CONFIDENTIALITY, DATA INTEGRITY

Computer scientists already had a rather rigid idea what security means long before the internet became ubiquitous and made its security an issue of political relevance.

'IT security' comprises of three main fundamental principles: availability, confidentiality and integrity of data. (Eckert, 2001) If these characteristics are ensured, IT security is achieved. Anything that might endanger one of these three principles, can considered to be an IT security risk. The logic of such a definition of IT security is that there never can be such a thing as IT security as a state as long as imperfection and faultiness exit in real-world IT systems. The same holds true not only for 'IT security', but also for 'internet security'. In computer science, the notion of 'IT security' and 'internet security' tend to be used synonymously.[1]

The existence of bugs in highly complex IT systems, the near-incomprehensible interdependency of sub-systemic components, incredibly sprawling fault-trees and potentially widely cascading effects do not only make ubiquitous availability, confidentiality and integrity of data wishful thinking. These factors also lay the theoretical seeds for discussions about a digital Pearl Harbour or a complete breakdown of the internet infrastructure, a discourse which has been around for more then ten years.

There are ways to link mere IT security problems to real-world problems. Whether an IT security risk actually requires some preventive or reactive actions depends on its respective prioritization by what is called risk management. IT risk management assesses potential IT security risks with a formula which equals a risk to the product of the amount of potential damages and the probability that these damages could actually happen. Security is turned into measurable, comparable figures, even though they might be based on weak epistemological foundations.

Internet security from a purely technical perspective has the tendency to become affixed with unachievable levels of availability, confidentiality and integrity of data, a perspective which loses sight of the actual importance of such data for societal actors. Technically insecure IT systems don't necessarily pose a security risk for users. They only do so if unavailability, non-confidentiality and non-integrity of technical systems has consequences for substantial interests of actors. The recursiveness of security is not the privilege of conceptualisations in computer science, it's linked to the basis of security per se.

[1]This statement is less a result of a study, which I would otherwise cite here, but rather a claim fed by empirical impressions. Cf. e.g. presentations and online lectures of ChristophMeinel, professor for computer sciences and CEO of the Hasso-Plattner-Institute, Potsdam, Germany (http://www.hpi.uni-potsdam.de/meinel/teaching/lectures_classes/internet_security_bjut.html)

## 2.3. ASSURED STATE OF UNCONCERN

One of the richest discussions on security in general was launched by the student of Western social security politics, Franz Xaver Kaufmann, in the early 1970s. His problem was very similar to that of students of internet security governance: to understand and frame his field of research by defining the notion of security and to get a grip on the basic "concepts" in his field of research.

Looking at the social security politics in major Western countries in the 20th century, he observed an "amalgamation" of three distinct conceptualizations into one "complex idea of security"(Kaufmann, 1973, p. 201)[2].

Three competing normative ideas of security—"idées directrices" as Kaufmann called them with reference to French socio-linguists —merged into one thick, hyper-normative idea: First, a "retrospective idea of 'security' and 'feeling of being safe'" [Geborgenheit]. In this sense, security is produced by a comprehensive, static order with visible guarantors for the stability of humans' psyche. Times of rapid changes generated by technology produce the opposite of such an order. The second interpretation of security follows a "pragmatic idea of 'system security' as producible, predictable availability of means for any purposes". The third idea of security is framed as a "psychologic conception of 'self assurance' as leitmotif for subjective identity". (Kaufmann, 1973, p. 341)

Thereby, the concept of 'security' became a rather ambivalent and self-referential normative term in public and political discourses. "'Security' in its normative sense is the unity of the characteristics envisaged by the different meanings, i.e. the assuredness of the reliability of protection or risklessness and the hence resulting state of unconcern." (Kaufmann, 1973, p. 344) With this amalgamation of ideas and its self-referential character, 'security' has risen to a grand societal value during the last century with status and impact comparable to values like 'freedom', 'order' or 'peace'. (Kaufmann, 1973, p. 48)

There have recently been attempts to broaden 'internet security' and adapt its conceptualization to the breadth of 'security' in general. Bruce Schneier made a first valuable step by bringing in psychology and cognitive science to broaden our understanding of computer security, claiming that, "Security is both a feeling and a reality." (Schneier, 2008, p. 50) Similarly, Anderson and Moore have summed up recent discussions on the links between psychology and security and incorporated psychological aspects into internet security, identifying "inappropriate obedience" (sic!), flaws in security usability, cognitive biases and fear of uncertainty and

[2]Quotes in English of Kaufmann (1973) and other non-English citations have been translated by AS

unfamiliar risks as causes for security threats or their discursive creation. {Anderson 2007}

However, these attempts concentrate on the level of the user and don't affect the societal level as much as Kaufmanns conceptualisation as assured "state of unconcern" did. What these approaches naturally lack are the politics of internet security and core concepts of political analysis like interests, actors, ideas or power. The Kopenhagen School, on the other hand, incorporated the mass-pychological appeal, which Kaufmann had identified in the early 1970s, into their securitization model. Before I'll elaborate on political aspects of security, more light needs to be shed on technological security as the parent category of IT security.

### 2.4. HARMLESS AND RELIABLE

For the purpose of conceptualizing internet security, it is worthwhile to look at Kaufmann's ideas on *technical security*. In a *narrow sense*, 'technical security' refers to the technical means and their appropriate functioning. The focus is on the artifacts themselves and whether they technically work in the way they are supposed to work. In the *broader sense*, technical security refers to the security of technical human-artifact-systems, e.g. transport safety or industrial safety. (Kaufmann, 1973, p. 60) Similarly, sociology of technology dichotomizes between technology as technological artifacts and technology as socially embedded systems. (Fohler, 2003)

On another dimension, technical security of a technical means incorporates the idea of an 'assured state of unconcern' described above. Accordingly, technical security can be defined as a) the "*harmlessness* … of the usage of by itself dangerous technical means" or b) as the "*reliability* of its effects, its functional abilities, the predictability of its performance" (Kaufmann, 1973, p. 62). With the rise of modern technologies and their in-built complexities and their usage of massive physical power, harmlessness and reliability have become inseparable characteristics. Conveying this idea on internet security, it is clear that the Internet is "by itself" one of the least physically dangerous technologies in modern society. Threats and dangers only come from the indirect social consequences of the usage of the internet, not from the technological artifacts themselves. In this respect, the internet is very different from, say, nuclear power stations, automobiles or guns.

The *threats for security of a technology*, from which no physical dangers arise on the artifact level, can occur on its functional level. Kaufmann claims that "security of the technical system depends on the definitiveness of system purposes and computability of system relationships" (Kaufmann, 1973, p. 64). The consequences here are twofold. On the one hand—and this is a very 1970s and cybernetics inspired perspective on technology—technical security is restricted to self-adjustable, self-repairing or -containing technologies with superior complex data-loaded decision

making processes. For a technical system to be secure in this sense, it must be comprehensibly measurable, it must know and be able to interpret any possible situation and deduce possible corrective actions.[3] Secondly, technical security in this sense is somewhat limited to functionally static technologies, which the internet clearly is not, especially not on and above the application layer. Differently put, technical security threats could arise when the purposes of a system have changed in time. Such an understanding knots security with political and societal statics.

### 2.5. ORDER, BORDERS, FUNCTIONS, POWER

To further complete the dimensions of internet security, it is necessary to introduce the dimension of *political security*. Political security has in modern, western thinking been divided into different securities like: 'national security', 'international security', 'public security', 'external security', or 'internal security'. Usage, habitualness and definition of these terms can differ internationally and over time.

In the modern world, the politically relevant conceptualisation of security has traditionally been state-centric and affixed with borders, military and territories, a different trend could be observed since the mid-1980s and, most notably, after 1989. After the demise of the Soviet bloc and the end of the alleged threat of Communist world take-over, politicians and scientists started using the concept of security in an ever deeper and broader way. No longer was security confined to nation-states and military threats, but was used in contexts such as drug trafficking, organized crime, terrorism and attacks on information technology. New actors, new security threats and new forms of coordination started changing the international security politics. (Baldwin, 1995; Baldwin, 1997; Bendrath, 2007; Daase, 1991; Daase, 1993; summed up by Krahmann, 2005)

For students of internet governance, this state-remoteness doesn't come as much as a surprise as for former 'nuke counters' in security studies. The internet has traditionally been an infrastructure with relatively little regulation by the states. What's more interesting here, is the linkage between security and order.

In line with Hobbesian and static societal thinking, "the idea of 'public security contains the protection … of individuals from threats by other individuals, and also the reciprocal reliability among individuals, and thus the maintenance of the existing order, which guarantees the reliability and thereby trust and quiet." (Kaufmann, 1973, p. 55) The function of public security is to enforce reliability of inter-individual

[3] An arguable example of an implementation of this philosophy is the so-called computer priority in fly-by-wire steering systems of recent Airbus planes. Airbus assumes that flight management computers are better at massive measurement data processing in critical situations and should therefore have the power to overrule pilots' steering decisions.

agreements by staying on the sideline, ready to defend "contracts with the sword". Security is the guarantor for securing societal institutions and also functions as the guarantor of trust.

And there begins the reflexivity of security, i.e. the "securing of securities", "guarantees for the fulfillment of future obligations" (Kaufmann, 1973, pp. 55+56). In that sense, public security describes an instrumental act of securing individuals and goods, though in a reflexive way.

The second branch of political security is 'national security'. In the standard literature of Realism, national security has been defined more or less as the integrity of national borders, the bodies of the state and the autonomy of a nation and the endangerment thereof by external actors. (Bowling & Newburn, 2006, p. 4) With the reflexivity and normative elevation of security, national security has become concerned with "'securing security', i.e. the creation of an international 'system', in which certain possible courses for action would be excluded and thereby others be made supposable." (Kaufmann, 1973, p. 60)

But the most prominent feature of "national security" is that it is traditionally linked with existential problems, high urgency and questions of survival and therefore requires extraordinary coercive and intrusive powers. This feature combined with the problem if not impossibility to intersubjectively define security, has lead constructivists and Kopenhagen school aficionados to formulate their securitization model in which "security is what a political actor or a political entity labels as security in a particular situation" (Daase, 1993, p. 45).

Previous paragraphs and sections have shed some light on the empirical usage of and definitional approaches towards security. A scientifically useful conceptualization of security should include these empirics of security. The following section outlines the dimensions of security in a more rigid way.

### 2.6. DIMENSIONS OF SECURITY

Baldwin identifies six dimensions or "specifications" of security "that would facilitate in analysing the rationality of security policy" (1997): security beneficiaries, security objects, degree of security, security threats, security means, costs of security and security timeframe.[4]

[4]These seven nouns paraphrase the seven questions Baldwin has raised to identify the seven dimensions of security: 1) Security for whom? 2) Security for which values? 3) How much security? 4) From what threats 5) By what means? 6) At what costs? 7) In what time period? (Baldwin, 1997, pp. 12-17)

The dimension of *security beneficiaries* refers to the actors whose security is to be preserved or protected by security governance. For defining security in the field of international relations, these actors might be the international system, states or individuals. For 'internet security', this view on security is too state-centric, too non-technical and should be supplemented by businesses and civil society groups.

The dimension of *security values* refers to actors' values like physical safety, economic welfare, autonomy, psychological well-being, political independence, or absence of fear. While territorial integrity is unlikely a value to be protected in the domain of internet security, technical specifications need be added, among them information systems, functional reliability, data integrity. The value of a specific item of 'internet security' should not be prejudged by equating security with 'vital interests'.

The dimension of the *degree of security* refers to the extent in which security is achieved. This precludes the idea that the passage from security to insecurity is continuous, rather than binary, i.e. there can be less or more security instead of either security or insecurity. With pure security being unachievable (cf. the reciprocity of security mentioned above), a binary dichotomy between security and insecurity would render 'security' useless as an analytical concept and make it into an impractical normative utopia. However, the common usage of 'internet security' or 'information security' in business and politics sticks to the continuous idea. The question there is: How much should be spent on which degree of security?

The dimension of *security threats* refers to the actual threats that endanger security values. Threats can be linked to *threatening actors* and can either be caused by intended actions of political actors[5], by non-intended consequences of human actions. In short, a threat is an action, a process, a development or an event, caused either by human actions and/or by systemic interdependencies, that could or actually do endanger one or many security values. The semantic usage of 'security' sometimes refers to certain technical phenomena or artefacts as security threats (nuclear weapons, botnets). While these phenomena impose their destructive capacities onto security values only by human action and are thus only a *means for security threats*, their inherent capabilities and destructive or coercive potential can make them be perceived as threats in themselves.

The dimension of *means of security* refers to the means to protect endangered values or to contain or to neutralize a security threat. As to internet security, means can be technical in nature, organizational and legal or political — they can basically encompass any imaginable means to overcome any threat against any security

[5] A threat can be defined as "a conditional commitment to punish unless one's actions are met"(Baldwin, 1997, p. 15).

object. To the extent to which it is the result of deliberate political choice, the mode of security governance can be regarded as a means to provide security. And just like any other means, the mode of governance is connected to certain costs, assists certain values more that others and is linked to actors who provide means of security, quasi *security means provisioning actors*.

The dimension of *costs of security* refers to the opportunity costs for implementing means of securing security values, i.e. costs for not supporting values other than security. A normatively neutral conceptualization of security does not assume that security has to be achieved by whatever it takes. In real world politics, costs of security are linked with degree of security.

## 2.7. DEFINING INTERNET SECURITY

A precondition for defining *internet security* is to have a solid definition of the *internet*. Unlike 'internet security', the 'internet' has been solidly defined in previous articles. Leaning on the definitions of Solum[6] and Libicki[7], 'internet' can be defined as a global agglomeration of sub-networks, computing devices and components, which are directly or indirectly connected to one another via the Internet protocols, and, in a wider sense, the contents and semantics communicated in this network.[8]

Based on the discussions of security in the previous sections, Baldwin's definition of security as "low probability of damage to acquired values"[9] (Baldwin, 1997, p. 13), and the definition of *internet* mentioned above, *internet security* can be conceptualized in the following way:

In short, *internet security* is the low probability of damage to acquired *values*, which are based on the *internet* and are related to *beneficiaries*, with the aforementioned low probability of damages achieved by applying protecting *means* against *threats*.

---

[6] "The Internet is a global network of networks, with communication between networks enabled by a communications protocol suite, currently TCP/IP."(Solum, 2008, p. 48) "In the broad sense, the Internet is a complex entity that includes the hardware and software technical infrastructure, the applications, and the content that is communicated or generated using those applications"{Solum 2008@49}

[7] Cyberspace "can be characterized as an agglomeration of individual computing devices that are networked to one another (e.g., an office local-area network or a corporate wide-area network) and to the outside world"(Libicki, 2009, p. 6); "view it as consisting of three layers: the physical layer, a syntactic layer sitting above the physical, and a semantic layer sitting on top" {Libicki 2009@12}

[8] For a more extensive definition of 'internet' cf.Mathiason, Mueller, Klein, Holitscher & McKnight, 2004 and {*Mueller 2007}.

[9] While Baldwin doesn't define 'acquired values', his usage implies that values can refer to physical objects or to norms or ideas. 'Acquired' links the object, that is to be secured, to an actor.

More detailed, *internet security* is the low probability of damage to acquired *values* forming the *internet* (such as sub-networks, computing devices, components; integrity, availability, reliability of data) or based and depending on the *internet* (such as contents and semantics; economic welfare, autonomy, political independence), which are related to *beneficiaries* (such as individuals, states, social groups, businesses), with the aforementioned low probability of *damages* achieved by applying protecting *means* (either technical, organizational or political in nature) against *threats* (emerging from either malevolent or ignorant actors, from systemic constellations, technical phenomena or artefacts).

This conceptualization emphasizes the different facets of security and internet security. It also shows some interdependencies of the dimensions of internet security on the conceptual level. After this definitional review on security, the following sections will analyse the essence of security governance and, then, internet security governance.

## 3. SECURITY GOVERNANCE

### 3.1. FRAMEWORK FOR PLURALISING TRENDS

The concept of *internet security governance* hasn't acquired widespread usage in internet studies, so far. The reasons probably are that internet security has only recently become a widely discussed regulatory topic and, secondly, that the concept of security governance itself only is its infancy.

Traditionally, internet governance has been focussed on institutional fora like ICANN, WSIS or IGF. Students of these institutions, are open to the assumption that political issues could be regulated by actors others than states. In the field of security studies and police studies this has for long been an anathema. But recent trends in these fields have created the necessity for these disciplines to adapt their frameworks and incorporate actors and governance structures.

For researchers in the field of international relations, security governance is not just a concept that would name the governance of the security sector. The new realities of the post-1989 world called for a new term to describe "this delegation of authority and the outsourcing of public policy functions"(Krahmann, 2003, p. 11). But security governance is also used to label a framework to analyse security politics in the post-Cold War world. The core features of this framework are its inclusion of non-state actors, that it considers new governance structures such as networked cooperation, uses a broadened and widened concept of security and thus of security areas, and concentrates on security provisioning processes instead of focusing on security organisations and players. (Krahmann, 2003; Krahmann, 2005) Further elements of this overall 'pluralisation of security' processes are the "increased emphasis upon

'high policing'", "changed roles of law enforcement and security agencies", "a blurring of the boundaries between international security and domestic concerns of order maintenance", and a new idea of coercive policing accompanied by "securitization and militarization" of police forces and increasing convergence of police, military and intelligence. (Bowling & Newburn, 2006)

### 3.2. MODELS OF GOVERNANCE

One aspect of the pluralization of security governance is the broadened set of actors involved. In non-internet security areas, both domestic- and outward-bound, students of security learned that other actors aside from the classical state could be an agent of security. In these security areas, however, the state is still considered to be the most important actor in security governance, and state centrism understandably continues to be the main perspective. This is obviously the case in classifications of security governance by the scholar of security studies Christopher Daase, who categorises security governance into three categories: governance by government, governance without government, governance with government (Daase & Engert, 2008).

Such a simplistic categorisation might be helpful in security studies to understand the different nature of states worldwide and different ways of security provisioning in strong western-type democracies or in sub-Saharan or trans-Caucasian failed or struggling states. It might be helpful to categorise different security regimes in different global regions. And it might be helpful to differentiate between the state as the sole actor in security politics (by government), the state as the architect and sponsor of a security architecture, but not sole executor of security politics (with government) or the state being completely absent from any form of governance (without government).

As to the modes of governance, Internet security governance seems to be different from these classic domains of security. In a sense or for its splattered competencies, resources, formal responsibilities and informal distribution of power, it's more of futuristic model of governance or resembles the alleged new medievalism in governance more than the classical security fields.

In his article "Models of Internet Governance" Lawrence Solum classifies five ideal-type models of internet governance: governance by self-governance and spontaneous ordering, by transnational institutions and international organizations, by code and internet architecture, by national governments and law, by market regulation and economics, and, finally, by hybrid models. (Solum, 2008, pp. 56-87) His classification helps as an inspiration for a heuristic model to classify the institutions of internet security governance.

Solum classifies governance by different governing institutions. Analysts of security politics in the field of security studies always ask: security by whom and by what means. That is: who implements which means that foster security? Transferring and adapting these institutions to internet security governance, the following institutions might be enlisted.

#### 3.2.1. BY NATIONAL LAW AND GOVERNMENTS

According to Solum, "most Internet regulation is regulation by national governments of Internet-related activities", such as regulating access to content, establishing regulatory frameworks, weighing liabilities. Limits of national regulation appear in attempts of either regulating the internet architecture itself or of blocking access to online content. (Solum, 2008, p. 68) Non-democratic countries like China, some Arab autocracies, and even western parliamentary democracies have modified their 'national' DNS systems to allow centrally managed address blocking. Countries like Germany have set national internet centers to combine police and intelligence units to address security related internet issues.

#### 3.2.2. BY INTERNATIONAL ORGANISATIONS

When national laws and governments face problems with border-crossing reach, the common reaction has been to transfer regulatory authority to an international organisation. Many existing international organisation have initiated projects and established task forces for internet governance in general and internet security issues in particular. UN's IGF, a stream of internet security agendas from ITU, and European countries have even set up a dedicated agency, ENISA.

#### 3.2.3. BY TRANSNATIONAL INSTITUTIONS

Transnational or international institutions comprise various either formal or informal entities, such as international institutions with international legal personalities, clubs, committees, or communities. While in non-internet politics, most informal institutions are somehow linked and subject to control of larger organizations.[10] For internet governance in general, ICANN is the prime example of a transnational institution.

[10]Cf. "What do we consider to be an International Institution", Website Max-Planck Institute for Comparative Public Law and International Law, http://www.mpil.de/ww/de/pub/forschung/forschung_im_detail/projekte/transnat_mehrebenensysteme/ipa/international_institutions/definition_ii.cfm

#### 3.2.4. BY MARKETS AND ECONOMICS

This model of governance views internet security issues from a mere economic perspective, considering internet security as something that will by solved by supply and demand and prices. Scholars of internet security economics try to trace security non-optima back to markets, their potential failures e.g. like decoupling of problem ownership and distribution of liabilities. (Anderson & Moore, 2007; Anderson, Böhme, Clayton & Moore, 2008)

#### 3.2.5. BY CODE AND INTERNET ARCHITECTURE

A mode of governance that is per definition and by nature unique to the internet, is governance by code and architecture. In a sense, every technical approach to internet governance necessarily involves 'code', even though code would only seldom change the architecture of the internet. A network monitoring system that sniffs for exploitative IP packet headers in a network is written in any code and doesn't change the architecture of the internet, whereas a filtering software, added to DNS servers of major ISPs, does indeed change the non-discriminatory packet handling, which used to be a core feature of the internet. Given these technical facts, many, if not every technical enhancement or enforcement of internet security is implemented by change of code or architecture. In this sense, code and architecture are not modes, but rather means of governance. The striking effect of governance by code and architecture is inherent in its global reach, its – superficially, at least – independence of geography and national borders.

The regulatory effect of code and architecture is tellingly circumscribed by Lessig's famous "code is law" equation. Today's internet technical security problems like botnets are to some extent the result of architectural decisions made more than two decades ago. Not designed as a global mass communication system, transnational business platform and communicational hub for globally operating enterprises, the internet's core code and architecture (like DNS, TCP/IP) doesn't meet everyone's understanding of what internet security should be like.

#### 3.2.6. BY SPONTANEOUS ORDERING

The idea of governance by code and architecture concentrates on the means of governance, i.e. on code and architecture as a way to shape behaviour and outcomes. At the same time code and architecture by themselves can be the result of interest-driven political considerations.

This also applies to 'governance by spontaneous ordering', another mode of internet governance enumerated by Solum. Spontaneous ordering doesn't happen automatically; it is done by actors, following a set of rules, either implicit or explicit. For systems connected to the internet and internet security, it is the group of system operators and administrators (sometimes called 'sysops'), who can by technical-

administrative acts remove and exclude persons or code. As Johnson/Post have put it, "sysops, acting alone or collectively, have the power to banish those who commit wrongful acts online."(Johnson & Post, 1996, p. 1390) Spontaneous order or spontaneous securing of the internet is the result of cooperation amongst technical experts acting unsighted by the radar of political control. I would thus want to refer to this mode of governance of peer production of security.

Solum adds an economical argument why internet security (defined as non-access to forbidden content available online) is best achieved by these groups of independently acting administrators, and not by governments. For the latter, it has become all too difficult and costly to monitor and technically ban the online-availability of illegal content. New technologies such as DPI however have the potential to radically change the rules of the play. (Bendrath, 2009)

#### 3.2.7. BY SELF-GOVERNANCE

In earlier internet times, self-governance of the internet has been linked to organisations such as IETF, ISOC or to the institution of RFCs (Rasmussen, 2007). Some researchers would arguably subsume ICANN under this category (Solum, 2008). Less from an organisational and more from an institutional perspective, self-regulatory approaches include "social codes" like internal corporate rules, codes of conduct for business associations, contractual solutions in business networks, harmonisation by standardisation organisations and "technical codes" such as user self-help tools, negotiation-based codes or function-oriented sub-infrastructures for security or other purposes. (Bendrath, 2008) While the institutions and means of self-governance might be clear {\cf. discussion of self-governance in \Holitscher 2003@30-50}, one decisive practical and legitimatory problem of any self-governance approach is representation and the inclusiveness of those affected by governance.

'Self-governance' by definition implies and practically requires an identifiable entity, a 'self' that could govern its own issues by itself. For the internet, one could think of the notorious 'internet community' as the identity to govern itself. However, the functional spreading of the internet and the derived increase of stakeholders have amplified the problem of self-governance as it has become difficult to include all the stakeholders affected by internet security problems or by implemented means to overcome alleged internet security problems. The 'self' that will claim to govern itself very likely doesn't match the stakeholders of all the dimensions of internet security.

#### 3.2.8. BY HYBRID MODELS

The modes of governance described above are ideal-types that would rarely happen to describe the governance landscape in its entirety. The realities of internet security governance unsurprisingly resemble what Solum called a "hybrid model" and can

be defined as an "arrangement that combines transnational self-regulation on the one hand, and nation-state-based intergovernmental public regulation on the other hand, to produce a complex, multi-layered regime." (Bendrath, 2008, p. 196) An inclusive study on the empirics of internet security governance is published by the Dutch research institute TNO. (Bruce et al., 2005) The study gives an inclusive idea on the different modes of internet security governance and paints a broad picture of the empirics of internet security governance, the actors involved and their relationships.

However, internet governance studies have yet to explain the reasons of both the origins and the sustainability of distinct governance approaches within the hybrid realities, the respective contribution of these governance models to internet security and the interfaces between these modes of governance. One of the reasons why this hasn't yet been achieved is that the list of governance models is still incomplete. One of the models that hasn't yet been analyzed by internet governance studies is peer production of security.

#### 3.2.9. BY PEER PRODUCTION

It seems at first to be odd to subsume a mode of production under models of governance. However, 'governance' itself does not only refer to 'steering', but also to the rowing of internet. In more scientific terms, a mode of governance is characterized both by actors and institutions deciding on policy goals and distribution of resources to achieve these goals, but also by the actors, means and institutions that try to achieve these goals on a tactical and operational level.

Peer production describes an organizational form to collaboratively provide certain, mostly immaterial, goods and services. In contrast to hierarchical organizational forms such as commercial firms or government agencies, peer production is done by a network of loosely collaborating actors which are not steered and controlled by a central entity. It is "radically decentralized, collaborative, and nonproprietary; based on sharing resources and outputs among widely distributed, loosely connected individuals who cooperate with each other without relying on either market signals or managerial commands."(Benkler, 2006, p. 60)

New information technologies and forms of usage have led to the rise of unprecedentedly distributed forms of collaboration. Open source software development and community content production with wikipedia are the most prominent among several examples. (Cooper, 2006; Lakhani & Von Hippel, 2003; Shirky, 2005; Shirky, 2008; van Wendel de Joode, de Bruijn & van Eeten, 2003; Von Hippel, 2005; Von Hippel & Von Krogh, 2003) Well known examples of peer production are Wikipedia or the development of open-source software such as Linux or Apache.

On the spectrum of modes of production, peer production is located at one end and central dirigisme at the other extreme. The distinguishing features between these modes are distribution of power, the existence and centrality of command structures, the ability of the central authority to impose a division of labor on the constituents, the distribution and accessibility of knowledge and information.

Peer production is the extreme form of networked production. In networked production, goods and services are the result of collaboration among distributed, more or less independent and autonomous actors. (Benkler, 2006; Shirky, 2008) While networks simply refer to the existence of different nodal actors, peer production assumes a certain degree of equality among the actors.

Peer production of internet security refers to any process, activity, pre-product or supporting product or tool that is pursued or produced by peers, i.e. within a networked organizational form of actors with relatively similar power status and ownership of assets involved. Similar to the radically new economics of content-production and distribution on the internet, peer production of security *for* the internet is facilitated by relatively low costs of means to provide security and new ways of building trust *on* the internet.

### 3.3. NORMATIVE ASPECTS

Both security and policing studies analyze physical world phenomena. Often, though not always, threats to security emerge from physical force, security is defined by physical integrity of real humans, and means of securing are just like threats based on physical force. Normative governance questions are more pressing when it comes to real bodies. Not astonishingly, security and policing studies are greatly concerned about the normative effects of recent changes in security governance. Transparency, accountability and the degree of coercion are important variables for the rating of legitimacy of a governance approach.

#### 3.3.1. COERCION

Policing refers to activities of dedicated groups to provide security. Policing can resort to different means for security provisioning, ranging from normative recommendations, to law-backed behavioral prescription to coercive inhibiting of actions that are considered to be detrimental to security. Security provisioning can be imagined along an axis of increasing degrees of coercion, of increased use or threat of use of force. But what is force in internet security governance? While internet security surely can also provided by means executed in the physical world (like house search and arrest of a cybercrime suspect or the physical destruction of cyberwarfare control center), it also includes measures that both happen in the non-physical world and are coercive, i.e. they limit the options for actions and freedom of individuals or groups. Examples of non-physical coercion in internet security

provisioning are banning individuals from accessing the internet, blocking access to internet content, public blame & shame communication, denying access to certain internet-based services or by denying freedom of speech by permanent interception of communication.

Policing studies divide policing into consensual and more coercive ways of policing. One of the normatively fundamental questions following the pluralization of security governance is whether the consensual model of policing will further decline and give way to a more paternalistic, technocratic model of policing? (Bowling & Newburn, 2006, p. 31)

With the centralisation of force by and in modern nation states, the ultimate forces are concentrated in the hand of polices and militaries. Historically, forces for providing national security and forces for domestic order had been separated. Inbound security forces adhered – at least in Britain as Bowling tells – to what was called democratic and consensual policing. The elements of consensual policing are the visibility of police forces (by uniforms), minimal use of force and the characterisation of policemen as 'citizen in uniform'. The cause for this organisational split were the Napoleonic *muchards*, Fouché's ubiquitous spies. Formal police roles in state security had been established in Britain due to Irish terrorism in the 1880s. (Bowling & Newburn, 2006, p. 6) Police forces were then gradually militarized in equipment, training, and culture or military was brought in itself to bring down rallies and riots. With the Great War, Britain got it's domestic spying agencies, police acquired quasi-military responsibilities and paramilitary special police forces were established. (Bowling & Newburn, 2006)

The societal function of internet security provisioning forces, if I may label them in this way, will have an influence on the overall organisation of internet security governance. A countertrend might lie in increased partnership between police and community. (Bowling & Newburn, 2006, p. 31) But the question is whether this results in greater security for citizens by more effective and unintrusive cooperation or whether it will on the contrary result in increased intrusion of police into citizens' privacy or the intrusion of citizens into other citizens' privacy?

#### 3.3.2. LEGITIMACY, ACCOUNTABILITY, TRANSPARENCY

Intrusive and coercive actions need to be legitimized by an overwhelming necessity for action. Legitimacy comes from following defined procedures, from certain characteristics of actors and by certain outputs and payoffs. With new modes and ways of governance, new approaches for legitimizing security operations and coercive actions are needed.

In liberal-parliamentary democracies security politics have never had good legitimatory procedures. "The defence and security sectors have not historically

faced significant shareholder scrutiny." (Bryden & Caparini, 2007a, p. 16) The chain of legitimation from voters and citizens to those executing power is rather long, obscure and partly even covert. But while decisions and actions in state security services are somewhat intransparent, they are at least somewhat accountable as the chain of executive command always ends in the office of a minister of defense or of the interior.

The pluralisation of security governance obfuscates the accountability of actors involved in security provisioning. The rise of private actors raises questions of accountability, as private actors are primarily accountable to their customers and shareholders, not necessarily to the public. (Caparini, 2007, p. 272) The same holds true for internet security governance where private actors hold responsibilities for some security provisioning activities.

So how could legitimacy emerge from a mode of governance where private actors have the potential to or actually do coerce third parties or the public in the name of security? Legitimacy for private actors is transferred to them from elected state bodies by their "decision to privatise formerly governmental functions" (Caparini, 2007, p. 266; cf. also Ronit & Schneider, 1999). This way of legitimization however doesn't exist for internet security governance, as it has never been solely controlled by states; on the contrary, governance of this field was by and large developed in the absence of states.

The second stream of public legitimacy for private security actors comes from "recognition of expertise and knowledge."(Caparini, 2007, p. 266) This argument takes on the idea of 'output legitimacy' or legitimation of political actions by their good results independent of the procedures through which political decision making and its execution takes place. (Scharpf, 1998) Taking this idea to its extreme, it could serve as a legitimization for benevolent autocracies or any other form of non-democratic government and governance.

The third source of legitimacy for private security actors is to impose transparency and procedural standards. Security studies have identified a list of practical means to enhance transparency, such as licensing of companies and their services, establishing justiciability of offences committed by private actors, blacklisting malicious actors from public contracting, global enforcement of rules and norms by international organisations. (Bryden & Caparini, 2007a, p. 16)

While private security corporations and, even more so, private military corporations have amassed and use substantial means of coercion and force, private actors in internet security primarily use non-physical means. But given the increasing embeddedness of the internet into social practices of individuals and groups, the consequences of being digitally excluded, marginalized, isolated can be substantial. It remains to be seen whether and to what extent the coercive means of internet

security provisioning can be legitimized by practices used in non-internet security fields.

### 3.4. GOVERNANCE STRUCTURES AND PROCESSES

Security governance can be envisaged as a subconcept of security politik[11]. The latter includes all the aspects of politics, policy and polity. The notion of governance however accentuates a few features in security politics: the multipolarity and non-centrality of the actor dimension and the processes and institutions by which political interests and objectives are turned into political output.[12]

Daase had identified four main dimensions of security governance in general (2008): object of governance ("what is governed"), structure of actors ("who governs"), mode of cooperation ("how is governed"), compliance ("why do actors stick to agreements"). The question of compliance is the consequence of the lack of a central governing actor who has the means for enforcing agreements. These questions grossly meet the characteristics of security summed up in the sections on the conceptualization of internet security above.

One fundamental change, observed by security and policing studies, refers to the way in which security is actually provided. Multilateralization, transnationalization, privatization and the rise of networks are the terms used to label the ongoing changes of forms of governance. For scholars of internet governance such characteristics are very familiar. (Klein, 2004; Kleinwächter, 2006; Mathiason et al., 2004; Mueller, Mathiason & Klein, 2007) The very elements of the internet that cause the organizational problems for providing security, e.g. the number and divergent kind of actors involved, its transnational nature and technological characteristics, at the same time contribute to the emergence of new potentials for innovation in security governance and provisioning.

Policing studies have yielded a literature that focuses on security as a producible good. Security here is the result of different processes, sub-processes and tasks pursued by different actors, no matter if private or statist. (Bowling & Newburn, 2006; Bryden & Caparini, 2007b; Caparini, 2007; Hänggi, 2003; Kempa, Carrier, Wood & Shearing, 1999)

---

[11] In German, there are no equivalents for *politics*, *policy* and *polity*, there's just *Politik.*

[12] Cf. definitions of *governance* by Caparini, 2007, p. 269 and {*Krahmann 2003@11}. Also noteworthy: „…governance can be differentiated from government along seven dimensions: (1) geographical scope, (2) functional scope, (3) distribution of resources, (4) interests, (5) norms, (6) decision-making and (7) policy implementation" (Krahmann, 2003, p. 12)

## 3.5. DIMENSIONS OF INTERNET SECURITY GOVERNANCE

Security studies had long ago developed frameworks for analysing security politics. Security studies have brought forth not only the nowadays ubiquitous idea of securitization, but also finely grained lists of general properties and dimensions of security in political practice. (Baldwin, 1997; Buzan & de Wilde, 1998; Daase, 1993; Daase & Engert, 2008)

Based on these conceptualizations, a heuristic framework for analyzing internet security governance can be developed, which would include a range of variables that can be deduced from the discussions in the previous sections. It would depend on the actual research question, methodology and research strategy to identify those variables that need to be included in an actual study.

Internet security is defined by a set of characteristics, foremost acquired values, beneficiaries, means, threats, and costs. Governance is characterized by policy objectives, structures of actors and modes of cooperation. The following paragraphs will elaborate on these characteristics on an abstract level.

*Actors*

The analysis of internet security governance involves the examination of many types of actors. Per definition, governance lacks a single government in the centre, and this holds true for the empirics of internet security governance. (Bruce et al., 2005)

Actors can have different roles in internet security governance and with regard to security characteristics like values, threats and means. Roles can refer to the ownership of a security value, a means of threat or a means to secure; they can similarly refer to the actual control over these items; or, more vaguely, to the influence over them, such as the cause of a threat. As to the roles in governance in general, one can differentiate between 'rower' and 'steerer'. More detailed roles depend on the actual processes that are relevant for a concrete field of analysis.

An important characteristic of an actor in internet security governance is his or her geographic reach. Furthermore, actors are shaped by the resources they have at their disposal to play their respective role.

*Means*

In the definition of security, means refers to the means to secure a value, an endangered object. Means are characterized by their ownership, their controlling and owning actors, their costs, their geographic boundaries and the degree by which they help to counter threats and achieve security. Besides these means of security, means of threat support to endanger security values, and the same means may be used for both ends.

*Governance structures*

Governance structures— the constellation of actors, their roles and the nature of their instruments to govern—are part of any governance analysis. The governance structure can be regarded as a means of security, insofar it can be, albeit not always is (think of historic paths or decision deadlocks), the result of deliberate political decisions that prioritize either efficiency, effectiveness, transparency, legitimacy, participation or any other political objective.

Furthermore, the structure of internet governance is either characterized by consensus or by the imposition of measures and by hard or soft approaches to regulation.

Given the predominance of modern nation states in politics, the analysis of governance structures tends to circle around the question of the role of the state and the degree and character of government involvement.

*Security values*

Security values are at the core of security politics, describing what is endangered and need to be protected. Similar to means, security values are characterized by their ownership or appropriation, the actors controlling them, stakeholders, their costs, their geographic boundaries. A politically important quality of security values is its potential vitalness, i.e. whether and to which extend security is the linked to 'vital interests' such as physical and mental integrity or even to survival.

*Threats*

Threats are defined as a potential damage on security values, either due to a commitment by actors to punish in order to reach certain goals or as unintended yet potentially damaging side-effects of actors' activities, or by systemic development that cannot be linked to any actor. Threats are characterized by their causes, by actors that actually threaten, by owners and stakeholders of the means necessary for the threat, by geographic reach of the threat.

*Processes*

As the definitional focus of governance is on the actual processes—i.e. actors with roles producing series of events within institutions and with certain resources (Miebach, 2008)—to reach a given policy objective, the processes to secure internet related values are at the centrepiece of internet security governance analysis.

Internet security governance is made up of a set of processes, most notably those that are necessary to provide the means of securing values or, in short, to provide security.

With internet security being a service and a good (for a discussion on security as a good cf. Krahmann, 2008), it can be split up in processes, subprocesses, respective tasks, roles and responsibilities that are necessary to produce these goods. These

processes depend on the domain of internet security (e.g. phishing, critical information infrastructure protection or illegal contents) and, depending on that, how these humanly addressable security tasks can be accomplished. For example, security provisioning processes for content-related threats could entail the following processes: detecting, verifying, implementing (content-related: deleting, blocking, filtering, etc.; infrastructure-system-related: re-architect, redesign), forensics, sanctioning, controlling, intelligence, problem analysis and general strategy. For different internet security domains these processes will likely look different.

## 4. CONCLUSION

This paper has aimed at clarifying our understanding of internet security and its possible dimensions, characteristics and ways to define it. To achieve this goal, different conceptualizations of security in general were analyzed

As 'internet security' has a multitude of possible meanings, this paper argues for a precise conceptualization of 'internet security'. In respect of the breadth of the concept of security, the concept of internet security is necessarily a vague concept, that can describe a multitude of contradictory empirics. For this term to be interpersonally useful and scientifically precise, its distinct respective dimensions— listed and described in this paper— need to be clarified.

To analyze the internet security governance, recent trends in security governance were summarized. Security and policing studies stress the importance of understanding the legitimacy of governance approaches and therefore the need to analyze actual processes of security provisioning. The paper listed general modes of governance and identified the necessity to add peer production as a mode of internet security governance.

Internet security studies should provide insight into the advantages, limits and side effects of different modes of governance and should offer political guidance of the usefulness and applicability of modes of security governance. Currently, we can observe increased attempts of states to get into internet security governance in ways that might arguably enhance 'internet security', but do also come at a cost for other 'acquired values'. In order to assess the usefulness of a security governance approach, it needs to be related to the several dimensions of security, such as the values it helps to protect, the means it uses for that, the costs for applying these means, the costs for achieving a certain level of security and the costs for remaining at a certain level of insecurity, the main beneficiaries of a mode of security governance and the threats that are addressed by it. Different modes of security governance are likely to bring forward different characteristics of security while neglecting others.

Internet governance studies lack knowledge about how peer production of internet security works, how it relates to other modes of internet security governance and its contribution and limits to the provisioning of internet security governance. The conceptual frameworks described in this paper might contribute to these efforts.

## 5. BIBLIOGRAPHY


Anderson, R., & Moore, T. (2007). Information Security Economics—and Beyond. *Lecture Notes in Computer Science*, *4622*, 68.

Anderson, R., Böhme, R., Clayton, R., & Moore, T. (2008, February). *Security Economics and The Internal Market*. European Network and Information Security Agency (ENISA).

Baldwin, D. A. (1995). Security Studies and the End of the Cold War. *World Politics*, *48*, 117-141.

Baldwin, D. A. (1997). The Concept of Security. *Review of International Studies*, *1*, 5-26.

Bendrath, R. (2003). The American cyber-angst and the real world –- any link? In R. Latham (Ed.), *Bombs and bandwidth: The emerging relationship between IT and security.* (pp. 49-73). New York: New Press.

Bendrath, R. (2007). Der gläserne Bürger und der vorsorgliche Staat: Zum Verhältnis von Überwachung und Sicherheit in der Informationsgesellschaft . *Kommunikation@Gesellschaft*, *8*(7).

Bendrath, R. (2008). The Social and Technical Self-Governance of Privacy. In O. Dilling, M. Herberg, & G. Winter (Eds.), *Responsible Business? Self-Governance and the Law in Transnational Economic Transactions.* (pp. 183-224). Oxford, Portland, Or: Hart Publisher.

Bendrath, R. (2009, March 3). *Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection.* Paper prepared for the International Studies Annual Convention, New York City, 15-18 February 2009, Retrieved August 4, 2009, from http://userpage.fu-berlin.de/~bendrath/Paper_Ralf-Bendrath_DPI_v1-5.pdf

Benkler, Y. (2006). *The wealth of networks: how social production transforms markets and freedom.* Yale University Press.

Bowling, B., & Newburn, T. (2006). *Policing and National Security.* [Web] First Draft – Not for citation without authors' permission, presented at London-Columbia 'Police, Community and Rule of Law' workshop, London 16-17 March 2006, Retrieved April 24, 2009, from https://clearingatkings.com/content/1/c6/01/84/31/policingandnationalsecurity.pdf

Brown, I., & Marsden, C. T. (2007, November). Co-regulating Internet security: the London Action Plan. (Paper presented at Second Annual Symposium of GigaNet, Rio de Janeiro, Brazil). Retrieved December 10, 2008, from http://giganet.igloogroups.org/download/publiclibr/papers/ianbrown

Bruce, R., Dynes, S., Brechbuhl, H., Brown, B., Goetz, E., Verhoest, P., et al. (2005). *International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues*. TNO report 33680. Retrieved November 10, 2008, from http://www.comminit.com/en/node/219712/303

Bryden, A., & Caparini, M. (2007a). Approaching the Privatisation of Security from a Security Governance Perspective. In *Private Actors and Security Governance.* (pp. 3-19). Münster: Lit Verlag.

Bryden, A., & Caparini, M. (2007b). *Private Actors and Security Governance.* Münster: Lit Verlag.

Buzan, B., & de Wilde, J. (1998). *Security: a new framework for analysis.* Lynne Rienner Pub.

Caparini, M. (2007). Applying a Security Governance Perspective to the Privatisation of Security. In M. Caparini, & A. Bryden (Eds.), *Private Actors and Security Governance.* (pp. 263-82). Münster: Lit Verlag.

Cooper, M. (2006). From WiFI to WIKIS and Open Source: The Political Economy of Collaborative Production in the Digital Information Age. *Journal on Telecommunications & High Technology Law*, *5*, 125.

Daase, C. (1991). Der erweiterte Sicherheitsbegriff und die Diversifizierung amerikanischer Sicherheitsinteressen. *PVS*, *3*, 425-451.

Daase, C. (1993). Sicherheitspolitik und Vergesellschaftung. Ideen zur theoretischen Orientierung der Sicherheitspolitik. In S. Feske, C. Schmid, B. Moltmann, & C. Daase (Eds.), *Regionalisierung der Sicherheitspolitik. Tendenzen in den internationalen Beziehungen nach dem Ost.* (pp. 39-64). Baden-Baden: Nomos.

Daase, C., & Engert, S. (2008). Global Security Governance: Kritische Anmerkungen zur Effektivität und Legitimität neuer Formene der Sicherheitspolitik. In G. F. Schuppert, & M. Zürn (Eds.), *Governance in einer sich wandelnden Welt.* (pp. 475-98). Wiesbaden: Nomos.

Dunn Cavelty, M. (2007). Cyber-Terror – Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. *Jounal of Information Technology & Politics*, *4*(1), 19-36.

Eckert, C. (2001). *IT-Sicherheit. Konzept - Verfahren - Protokolle.* München: Oldenbourg.

Fohler, S. (2003). *Techniktheorien. Der Platz der Dinge in der Welt der Menschen.* München: Fink.

Hänggi, H. (2003). Making Sense of Security Sector Governance. *Challenges of Security Sector Governance. Münster: Lit Verlag*, 3-22.

International Telecommunications Union (2005, June). A Comparative Analysis of Cybersecurity Initiatives Worldwide. (WSIS Thematic Meeting on Cybersecurity, Geneva, Document CYB/05).

Johnson, D. R., & Post, D. (1996). Law and Borders: The Rise of Law in Cyberspace. *Stanford Law Review*, *48*(5), 1367-1402.

Kaufmann, F. X. (1973). *Sicherheit als soziologisches und sozialpolitisches Problem: Untersuchungen zu einer Wertidee hochdifferenzierter Gesellschaften* (2., umgearb. Aufl. ed.). Stuttgart: Ferdinand Enke Verlag.

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.

Klein, H. (2004). Understanding WSIS: An institutional analysis of the UN World Summit on the Information Society. *Information Technologies and International Development*, *1*(3-4), 3-13.

Kleinwächter, W. (2006). Internet Co-governance: towards a multilayer multiplayer mechanism of consultation, coordination and cooperation (M3C3). *E-Learning*, *3*(3), 473-487.

Krahmann, E. (2003). Conceptualizing Security Governance. *Cooperation and Conflict*, *38*(1), 5. Retrieved April 6, 2009, from the Sage database, http://cac.sagepub.com/cgi/content/abstract/38/1/5

Krahmann, E. (2005). Security Governance and Networks: New Theoretical Perspectives in Transatlantic Security. *Cambridge Review of International Affairs*, *18*(1), 15-30.

Krahmann, E. (2008). Security: Collective Good or Commodity?. *European Journal of International Relations*, *14*(3), 379.

Lakhani, K. R., & Von Hippel, E. (2003). How open source software works: 'free' user-to-user assistance. *Research Policy*, *32*(6), 923-943.

Libicki (2009). *Cyberdeterrence and Cyberwar.* RAND.

Mathiason, Mueller, Klein, Holitscher, & McKnight (2004, September 9). *Internet Governance: The State of Play* . Retrieved February 23, 2008, from http://www.internetgovernance.org/pdf/ig-sop-final.pdf

Miebach, B. (2008). Prozesse. In N. Baur (Ed.), *Handbuch Soziologie.* (pp. 373-90). Wiesbaden: VS Verlag.

Mueller, M., Mathiason, J., & Klein, H. (2007). The Internet and global governance: Principles and norms for a new regime. *Global Governance: A Review of Multilateralism and International Organizations*, *13*(2), 237-254.

Rasmussen, T. (2007, October). *Techno-politics, Internet Governance and some Challenges Facing the Internet*. Oxford Internet Institute, Research Report 15. Retrieved December 12, 2008, from http://www.oii.ox.ac.uk/research/publications/RR15.pdf

Ronit, K., & Schneider, V. (1999). Global Governance through Private Organizations. *Governance*, *12*(3), 243-266.

Scharpf, F. W. (1998). Demokratie in der transnationalen Politik. *Internationale Wirtschaft, Nationale Demokratie. Herausforderungen Für die Demokratietheorie*, 151-174.

Schneier, B. (2008). The Psychology of Security. In S. Vaudenay (Ed.), *Progress in Cryptology-Africacrypt 2008: First International Conference on Cryptology in Africa, Casablanca, Morocco, June 11-14, 2008, Proceedings.* Springer. Retrieved 2008, from the Google Scholar database, http://www.schneier.com/paper-psychology-of-security.pdf

Shirky, C. (2005). Epilogue: Open Source Outside the Domain of Software. *Perspectives on Free and Open Source Software*, 483-488.

Shirky, C. (2008). *Here comes everybody: the power of organizing without organizations.* Penguin Press HC, The.

Solum, L. B. (2008). Models of Internet Governance. *Illinois Public Law Research Paper No. 07-25.* Retrieved December 10, 2008, from http://ssrn.com/abstract=1136825

van Wendel de Joode, D. J. R. V., de Bruijn, J. A., & van Eeten, M. J. G. V. (2003). *Protecting the virtual commons. Self-Organizing Open Source and Free Software Communities and Innovative Intellectual Property Regimes.* The Hague: T.M.C. Asser Press.

Von Hippel, E. (2005). Open source software projects as user innovation networks. *Perspectives on Free and Open Source Software*, 267-278.

Von Hippel, E., & Von Krogh, G. (2003). Open source software and the" private-collective" innovation model: Issues for organization science. *Organization Science*, 209-223.

Wilson, C. (2007). *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.* Congressional Research Service. CRS Report for Congress.