International
Studies
Review

International Studies Review (2013) **15**, 86–104

Internet Security and Networked Governance in International Relations[1]

Milton Mueller
Syracuse University

Andreas Schmidt
Delft University of Technology

and

Brenden Kuerbis
University of Toronto, Syracuse University

This paper asks whether the Internet's heavy reliance on nonhierarchical, networked forms of governance is compatible with growing concerns about cyber-security from traditional state actors. Networked governance is defined as a semipermanent, voluntary negotiation system that allows interdependent actors to opt for collaboration or unilateral action in the absence of an overarching authority. Two case studies—Internet routing security and the response to a large-scale botnet known as Conficker—show the prevalence of networked governance on the Internet and provide insight into its strengths and limitations. The paper concludes that both cases raise doubts about the claim that introducing security concerns into Internet governance necessarily leads to more hierarchy and/or a greater role for governments.

Internet governance is now one of the most lively and important topics in International Relations (IR). No aspect of Internet use is more significant to the field of IR than its intersection with security issues. In both developed and developing countries, some national security advocates are emphasizing the need for extraordinary changes in Internet policy and governance to deal with the problems of cyber-crime, cyber-war and -terrorism, cyber-espionage, and the security of "critical infrastructures" (Dunn Cavelty 2008, 2013; Nye 2011; Clark and Landau 2011; Deibert and Crete-Nishihata forthcoming).

This paper argues that understanding Internet governance—both its current reality and its future prospects—requires IR scholars to test and extend their theories of global governance, especially as they apply to cyber-security. In particular, a more robust, clearly defined concept of *networked governance* is needed, yet is missing from the dialogue. It is true that a growing number of IR scholars are

[1]Paper prepared for the ISA Presidential Panels on International Relations in the Information Age, March 31, 2012, San Diego, California. Version 2.0 (May 15, 2012) revised based on workshop comments; version 3.0 (September 30, 2012) revised based on anonymous reviewer comments. Version 4.0 (November 20, 2012) based on additional comments.

Mueller, Milton, Andreas Schmidt, and Brenden Kuerbis. (2013) Internet Security and Networked Governance in International Relations. *International Studies Review*, doi: 10.1111/misr.12024

invoking network-related concepts and methods (Kahler 2009). But there are two problems with this corpus.

First, much of what is called the network literature in political science and IR hinges on the use of mathematical network analysis techniques. While those techniques can be useful, it is important to differentiate that literature from research based on "the network" as a theory of organization or governance. Although the two can overlap—and are often confused—they are not the same. An approach to social networks that focuses on mapping out links and nodes does not necessarily contribute anything to our understanding of the role of state-imposed hierarchies in global communications governance, the topic with which this paper is concerned.

Second, the IR literature that does speak to network organization (for example, Slaughter 1997, 2004; Eilstrup-Sangiovanni 2009) has never applied the concept to the governance of the Internet. This is likely due to the IR field's general unfamiliarity with the operational details of the Internet. And yet networked governance is the native form of global Internet governance and still constitutes the norm rather than the exception in key aspects of its operations. We would go further and assert that this reliance on looser forms of governance is a major factor in many of the policy controversies around the Internet. When national security experts complain that "feeble governance structures" make it difficult to execute cyber-security strategies,[2] the real target of their complaint, in our view, is the Internet's reliance on nonhierarchical forms of governance.

If networked governance is endemic to the Internet and states generally rely on hierarchy in security matters, questions about the compatibility of the two become salient. Providing security and the control of legitimate force have been the essence of the modern nation-state and differentiate a functioning from a failed state. While some research suggests that nonstate actors are responsible for a growing share of the overall security production process (Krahmann 2010, 2005; Bryden and Caparini 2006), in cyber-security nonstate actors already dominate security provisioning. The paper is thus concerned with two questions:

a) Is the Internet's heavy reliance on networked forms of governance and nonstate actors compatible with concerns about cyber-security from state actors?
b) Are hierarchically organized nation-states *conflicting* with the operationally decentralized, networked form of organization found on the Internet, or are they *adapting* to it?

In this paper, we use a structured, focused comparison method to address these questions.

The paper is organized as follows. The first section critically examines the progeny and use of network theories of organization. The discussion is intended to clarify what is meant by networked governance when applied to IR and to cut through some of the confusion caused by overuse or imprecise application of the "network" concept in social science.

The second section is empirical and examines two cases of networked governance on the Internet: (i) the organization of Internet routing; and (ii) the organization of Internet service providers and other actors in the response to a global security incident, the Conficker worm.

The third section draws on the previous material to address the research questions and to make a more general argument that networked governance on the Internet—which is undertheorized and inadequately researched empirically—

[2]Quoting John Lewis of Washington's Center for Strategic and International Studies in "Feeble Governance? The Push to Discredit Multistakeholder Institutions," Internet Governance Project blog, April 18, 2012. http://www.internetgovernance.org/2012/04/18/feeble-governance-the-push-to-discredit-multistakeholder-institutions/.

needs to be better recognized and understood before any political interventions to change it are made.

Networks, Theory, and Method

The term *network* invokes a confusing thicket of concepts and literatures in the social sciences.[3] Anyone using it must first clarify and differentiate the diverse strands of theory and modes of analysis involved (Knox et al. 2006; Boerzel 1998; Mueller 2010).

Markets and Hierarchies and...?

Representations of social relations as networks have been around for a long time. The idea of the network as a distinct organizational form or mode of governance, on the other hand, is relatively recent in the overall history of network ideas. It emerged in the late 1980s and early 1990s as a new twist to the dominant theory of economic organization known as the *theory of the firm* (Williamson 1975, 1985). Firms or hierarchies were defined as organizations subject to a division of labor defined and imposed upon the constituent elements by a manager(s) with the authority to make binding decisions. Their counterpart was *markets*, wherein resources or inputs were acquired by buying them from whatever external firms or individuals offered them at the best price at the moment. Oliver Williamson's canonical theory attempted to explain which aspects of economic production would be internalized by firms (hierarchies) and which would be governed by means of market transactions and the price system. The key explanatory variable in this approach was the transaction cost; that is, the cost of search, negotiation, and enforcement of exchange agreements (Coase 1937, 1960). If the transaction costs could be minimized by bringing a particular stage of production into the hierarchical arrangements of the firm, then that organizational form would prevail; if not, there would be reliance on markets.

In the 1980s, theorists began to observe looser affiliations among multiple firms—outsourcing, franchising, research alliances, and other semiautonomous relations—and to discuss how this phenomenon fits into the market-hierarchy framework. The initial tendency was to describe them as hybrids located somewhere "between markets and hierarchies" (Thorelli 1986). But in 1990, sociologist Walter Powell published a famous paper advocating a clean break with firm theory (Powell 1990). Powell contended that networks constituted a distinctive organizational form that was "neither market nor hierarchy." A network was said to be based on *the relationship* rather than *the transaction*; it was composed of longer-term bonds of reciprocity among economic actors that were too stable to be classified as market transactions and too loose to be classified as formal hierarchies. Networks were characterized as relying on lateral as opposed to hierarchical channels of communication, which made it possible to more efficiently exploit complementary skills and knowledge dispersed among multiple actors.

Note Powell's emphatic insistence that the organizational form he was discussing was *neither* market *nor* hierarchy and thus was outside the framework of transaction cost economics (TCE). Indeed, an important precursor to Powell's intervention was Granovetter's (1985) sociological critique of TCE-based theories of economic organization. Granovetter argued for the "embeddedness of economic behavior"; economic actors are heavily constrained by ongoing social relations and not just by rational calculations regarding cost. Thus, there was (and may still be) an unresolved tension in the theory of networked governance. The

[3]Knox, Savage, and Harvey (2006:114) make the ironic observation that "network ideas are remarkably poorly networked among themselves, with very little dialogue between different traditions of network thinking."

older, TCE-based theory of the firm provided a theoretically integrated explanation of how markets and firms were interdependent and why any given industry produced a specific distribution of organizations along the market-hierarchy spectrum. Organizational sociology, on the other hand, emphasized the embeddedness of actors in a network of social relations based on reciprocity and trust.

Network as Form of Organization

By the late 1990s, however, this tension seems to have disappeared, perhaps because social embeddedness can be seen as a way of reducing transaction costs. It became common to view networks not as an alternative paradigm to markets and hierarchies, but as one of the three basic modes of economic organization (Thompson 2003). Reflecting this consensus, Jones, Hesterly, and Borgatti attempted to define a "general theory of networked governance," claiming a "synthesis" of transaction cost theories and social network theories of economic organization (1997:913). A dominant view of network governance emerged as "flows of resources among nonhierarchical clusters of organizations made up of legally separate units" (1997:914). The network organization, they claimed, is a response to exchange conditions which drive firms toward structurally embedding their transactions. While TCE can illuminate these conditions, it is inadequate by itself because it focuses only on dyadic relations and does not take account of other ties actors might have. A synthesis of sociological and TCE-based approaches best explains networked governance, they claimed.

A useful crystallization of the concept of networked governance comes from the German political scientist Fritz Scharpf (1993, 1997). Scharpf speaks of networks as "voluntary negotiation systems in which partners are free to choose between negotiations and unilateral action" (1997:143). Networks are conceived as "a semipermanent structure within which individual interactions are embedded"; they involve the "memory of past encounters" and the "expectation of future dealings."[4] Networks can be characterized as a form of governance, insofar as affording private actors the freedom to choose between negotiations, and unilateral action reflects a conscious policy decision or an act of forbearance by authorities; it could also arise due to the inability of any entity to establish hierarchical authority over a certain domain of activity.

It should be emphasized that networks, hierarchies, and markets are not mutually exclusive categories that exist in isolation from each other. In many descriptions of networked organizations, it is, after all, (hierarchical) firms or organizations that constitute the units of the network. Moreover, whether one is dealing with firms or networks, market prices and market-based contractual negotiations play a powerful role in setting the parameters that shape networks' and organizations' interactions. One should view networked organizations as a particular organizational form that arises within a broader ecosystem of social relations.

Networks and IR

Many political scientists (for example, Fung, Russon Gilman, and Shkabatur 2013 in this issue) still confine their understanding of Internet-enabled networks to national institutional frameworks. But the idea of network governance has

[4]This topic exhibits the regrettable tendency of contemporary social science to proliferate and market dozens of labels for the same concept. Adler (2001), for example, counterposes markets, hierarchies, and "trust-" or "community-" based organizations; Benkler (2006) refers to "peer production"; Howard (2006) prefers the term "heterarchy," but defines it in a way that closely parallels Jones, Hesterly, and Borgatti 1997's definition of networked governance.

proved especially useful in studying transnational orders. In a globalizing economy, the existence of fragmented, competing sovereigns undermines the ability to create simple command hierarchies or clear principal–agent relations among transnational actors, creating a fertile space for the emergence of alternative, looser forms of organization (Schneider and Werle 1991; Dean, Anderson, and Lovink 2006). In an argument that parallels Powell's justification of networks in business, Reinicke (1997) characterized "global public policy networks" as a new way of mobilizing resources that are widely dispersed across public and private actors, and as a means of generating the consensus and legitimacy needed to develop and implement policy. Similarly, Singh (2013) stresses the influence of transnational communicative networks on shaping ideas about and thereby the agenda of global politics.

American scholars led by Slaughter (1997, 2004) and Raustiala (2002) began to highlight the importance of the so-called *transgovernmental networks* (TGNs)—international information exchange and cooperation among lower-level government agencies on common problems without formally negotiated treaties. Empirical research by Eilstrup-Sangiovanni (2009) shows that governments are strategic in deciding whether to form TGNs or to push for more binding, hierarchical forms of international cooperation. Closely related to the idea of TGNs is the European view of governance networks advanced by Kooiman (2003) and Sørenson and Torfing (2007). In these applications, the links to Powell, Scharpf, and organizational theory are evident.

Networks and Power

An earlier, somewhat naive view of networks tended to see them as flat, intrinsically egalitarian modes of organization. That is now being replaced by a more nuanced understanding of the way network structures create or distribute power among actors (Kahler 2009). Specifically, economists have long recognized the presence of network externalities, which create greater value as more actors converge on the same network because of demand-side economies of scope (Rohlfs 1974; Economides 1996). Network externalities can give larger, established networks both inertial power and the power to exclude (Cowhey and Mueller 2009). Some actors are in a better position to create the critical mass required to get a viable network off the ground. Drezner's (2007) concept of "club governance," which emphasizes the ability of alliances among a few key state actors to shape global governance, has some similarities to the concept of critical mass in network economics. Actors positioned more centrally within networks, or who seize a first-mover advantage, may be better able to influence the information flows within it (Wong and Lake 2009).

Unresolved Issues

While the concept of networked governance has theoretical and empirical substance, there are still ambiguities surrounding it. One big source of confusion comes from our enhanced ability to represent social relations (or anything else) as networks using graphs and related mathematical techniques. The increasingly popular use of network representations in political science, while constituting an important addition to researchers' toolbox in some respects, gives them the ability to find "networks" wherever and whenever they want. If one looks at the bulk of recent scholarship invoking "networks" in IR and political science, one finds that the subject is usually not a specific mode of organization or governance, but the arbitrary definition of some kind of entity as a node and an arbitrary designation of some kind of relationship between them as a link, followed by the use of graphs and some mathematical analysis of the network model so constructed

(Hafner-Burton, Kahler, and Montgomery 2009; Ohanyan 2009; Dorussen and Ward 2008; Maoz, Terris, Kuperman, and Talmund 2003). The issue of organizational form may or may not be part of the analysis; usually, it is not. Our ability to represent social relations as networks must not be confused with the presence of networked governance as defined above.

The most important unresolved issues, however, involve the relationship between states and networked governance in transnational forms of organization. Most IR applications of the network organization concept have focused on state actors, or networks within institutional frameworks defined through hierarchical action by states, such as TGNs. These state-centric approaches do not come to grips with the key questions relevant to Internet governance: Is networked governance of the Internet a stable, continuous form of organization, or merely something that temporarily fills a vacuum left by the absence of established hierarchy or hegemony? Does the current dominance of private actors in transnational Internet governance permanently alter the nature of state authority in global communications, or is it a temporary episode?

Method

As noted in the introduction, we use a structured, focused comparison method involving two cases of Internet security governance (George and Bennett 2005). The first is the security of Internet routing, and the second involves a response to a major botnet. Both cases are similar in that they involve security threats that are global in scale and affect the functionality of core Internet infrastructure. The cases differ in that one involves efforts to deal with a background vulnerability (BGP route hijacks) that is a well-known, long-term feature of Internet routing protocols. The other case, the Conficker botnet, constituted a distinct event, an aggressive new type of hack that created one of the largest botnets ever with the capability of supporting major denial of service attacks or cyber-crime delivery. The cases thus represent two distinct types of threats. Together, they cover the most common types of security problems, but not all types. One might expect to see different kinds of state responses to these two basic threat types because one requires standards revision and the other requires an immediate, emergency response.

We review these two case studies to assess a) the compatibility of networked Internet governance with states' security concerns and b) how states adapt to the prevalence of networked governance on the Internet. Ultimately, we find that despite the major differences in the type of threat involved, states responded similarly—by adapting to networked governance rather than changing it.

The Internet and Networked Governance

This section examines the role of networked governance in managing two types of security problems on the global Internet: routing security and incident response. We focus primarily on the actions and policies of network operators, the organizational entities who actually produce Internet service, and which do most of the work of Internet security production.

Routing Security

Routing is one of the most fundamental aspects of Internet operations: It is the process by which information packets are guided from their origin to their destination by "hopping" from one network to another. An *autonomous system* (AS) is the basic unit of routing policy on the Internet. It refers to a single network, or a group of networks, controlled by a common administrator(s) on

behalf of a single administrative entity (such as a university, a business, or a business division). The primary "law" or rule set that governs Internet routing is a technical standard for communication among routers known as Border Gateway Protocol (BGP). BGP was developed by the Internet Engineering Task Force (IETF), a transnational, private-sector standards development organization.

Internet routing is itself a form of networked governance. Multiple operators of ASs coordinate their actions to produce global connectivity, but each one is free to define its own policies and make its own decisions about what other operators' routing announcements are and which packets it will accept or reject. The IETF has no hierarchical authority over operators; insofar as they adhere to BGP and other relevant standards, operators do so voluntarily in order to maintain compatibility with their communication partners. Abuses and misbehavior are sanctioned primarily by an individual operator's decision to block routes and networks associated with malfeasance. Routing policies and practices *as a whole* are not subject to the hierarchical regulation of a single authority. True, each operator has some kind of nexus with one or more legal jurisdiction, but there is no national or transnational system of regulation that directly intervenes in routing as such.

Border Gateway Protocol is subject to known security vulnerabilities (Butler, Farley, McDaniel, and Rexford 2010). One of them, known as "prefix hijacking" or "route leaks," allows an AS to propagate routing information that affects networks over which it has no real authority or management responsibility, thus diverting traffic from its intended destination. Prefix hijacking can occur deliberately, but more often it occurs due to configuration errors by network operators. In February 2008, for example, the government of Pakistan ordered Pakistan Telecom to block access to YouTube locally. Pakistan Telecom dutifully advertised a route to its upstream international connectivity provider that would discard all packets headed from YouTube to its network. This instruction was not defined at the correct level of specificity, however, and the upstream provider mistakenly propagated the bogus route throughout the world routing system. This led to a global inability to access YouTube. The problem was detected by the YouTube staff and, with cooperation from other operators, normal service was restored after 30 minutes to 2 hours, depending upon where one was located on the Internet.

Another famous route hijack took place in April 2010, when a configuration error by China Telecom advertised routes that included a large number of route prefixes in the United States and Europe that China Telecom was not authorized to service. News of this incident inflamed US–China relations when the US–China Economic and Security Review Commission issued a report to Congress in November 2010 claiming that China had "hijacked massive volumes of Internet traffic" by using the routing system to "instruct U.S. and other foreign Internet traffic to travel through Chinese servers" (USCESRC 2010:243–244). While most of the Internet ignored the route leak because of their filtering policies (Labovitz 2010), the incident underscored BGP's vulnerabilities—and the way interstate tensions might exacerbate the security concerns associated with such vulnerabilities.

The main routing security tool that exists now follows a highly decentralized, voluntaristic networked governance model: ISPs individually "filter" routes based on information about updates and announcement messages from trusted peers. Internet Routing Registries (IRRs) were created to make this form of filtering scalable. IRRs are open data repositories that allow network operators to register their own routing policies and to look up the routing policies of other network operators (Bates, Gerich, Joncheray, Jouanigot, Karrenberg, Terpstra, and Yu 1995). According to MERIT Networks, there are currently more than 30 IRR operators mirroring over 70 Routing Policy Repositories.

Figure 1 is a visualization of the IRR system of security production as a network graph. Operators of IRRs are represented by circle nodes, and Routing Policy Repositories are represented by square nodes. When an IRR mirrors a Routing Policy Repository, the visualization shows an outward link pointing from the IRR node to the Repository node it mirrors. The square nodes (Repositories) are sized by in-degree (that is, the number of links pointing to it). The largest square in the graph is the Route Arbiter Database (RADb) operated by MERIT Networks.

The IRR system has been used to build satisfactory tools for detecting erroneous and suspicious routing behaviors (Siganos and Faloutsos 2007; Sriram, Borchert, Kim, Gleichmann, and Montgomery 2009). Nevertheless, there is dissatisfaction with the degree of routing security produced. Many of the critiques focus on the inconsistent use, variable policies, and lack of authentication of the information contained in them (Huston 2009). Their reliance on voluntarily transmitted updates of policy information is alleged to have produced incomplete or obsolete data (ENISA 2010; Siganos and Faloutsos 2004).

Over the last decade, a more radical effort to improve routing security has been proposed. It is known as the Resource Public Key Infrastructure (RPKI). RPKI is a specialized public key infrastructure (PKI) that uses cryptographic techniques to secure addressing and routing infrastructure. The intent of the RPKI is to support a hierarchy of X.509-based certificates that allow relying parties to automatically validate assertions about who is authorized to use specific IP addresses and autonomous system (AS) numbers in routing announcements.

A critical fact about the RPKI is that the issuance of security certificates would be tied directly to the issuance of Internet protocol (IP) addresses. IP addresses, the unique numbers that define a node on the Internet, are allocated by means of a global hierarchy that starts with the Internet Assigned Numbers Authority (IANA) of ICANN. While ICANN is a private actor, its IANA function is controlled contractually by the US government. The IANA allocates large address blocks to regional address registries for the Americas (ARIN), Europe

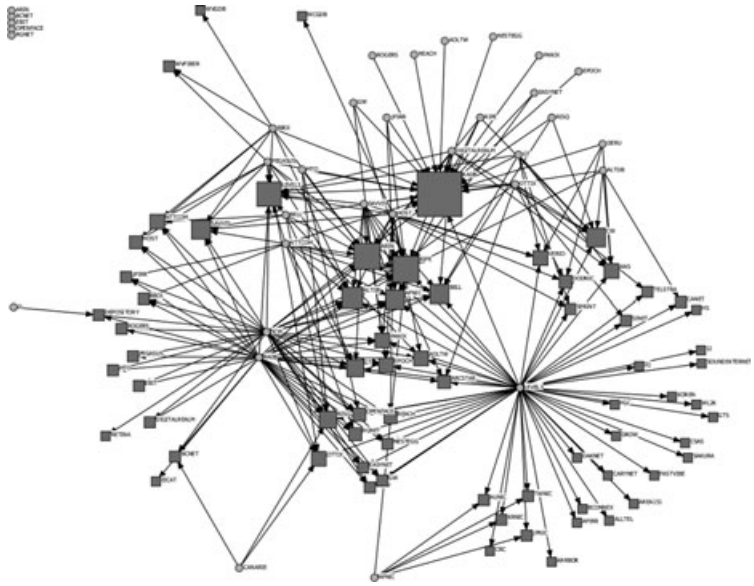

Fig 1. Internet Routing Registries (circles) and Mirrored Routing Policy Data Repositories (squares), Square Nodes sized by In-degree

(RIPE-NCC), Latin America (LACNIC), Asia Pacific (APNIC), and Africa (AFRINIC). These regional Internet address registries in turn allocate and assign smaller IP address blocks to commercial Internet service providers or to specific organizations, which in turn may assign them to end users in various ways (Figure 2).

The RPKI would enable the legitimate holder of an IP address block to authorize (by creating a certificate) what route announcements could be originated from that block. A relying network operator could then use a chain of valid certificates, starting from a known trust anchor and moving down the hierarchy to the user, to determine whether a route announcement had been authorized by the legitimate holder of the IP address block. The RPKI is thus a hierarchical system of validation. From the standpoint of TCE, it is an attempt to create an authoritative hierarchy over routing information in order to minimize the transaction costs associated with having thousands of operators validating routing information on a pairwise basis using a decentralized network of IRRs.

Much of the impetus for this proposed deviation from networked governance has come from the US government. The RPKI emerged from research funded by the National Security Agency and DARPA to address routing security problems (Kent, Lynn, and Seo 2000). Individuals affiliated with US government contractor BBN Technologies authored Internet drafts proposing to use digital certificates to authenticate IP addresses, AS identifiers, and BGP announcements (Seo, Lynn, and Kent 2001). Later, the Department of Homeland Security funded efforts to take this work into the IETF standards arena and into the regional Internet registries. More recently, the Federal Communications Commission's Communications Security, Reliability and Interoperability Council (CSRIC) sponsored a Working Group involving ISPs, equipment manufacturers, service providers such as Google, computer scientists, and law enforcement to develop a "framework" (as opposed to a regulatory policy) that would encourage RPKI adoption.[5]

But the potentially hierarchical and authoritative nature of RPKI has created obstacles to its acceptance and implementation. Tying certificate issuance to the address allocation hierarchy could convey substantial regulatory power to the

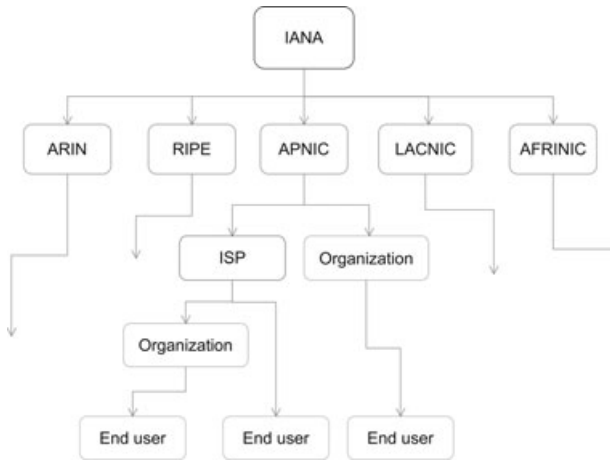

Fig 2. The Internet Protocol Address Allocation Hierarchy

[5]See the composition of Working Group 6 of the Communications Security, Reliability and Interoperability Council. http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iii.

top-level address allocation authority. Whoever issues the certificate at the trust anchor may gain significant power over entities using certificates below them in the hierarchy, as that authority would be able to revoke the certificate or attach conditions to its use. Revoking the certificate could prevent validation of route announcements and thus disable a network operator's routing. Either the IANA or the regional address registries, or a combination of both, could gain substantial authority over network operators. Thus, while most regional Internet address registries have launched resource certification and validation services, they have been unable to develop policies governing the issuance of resource certificates that enjoy strong support from network operators (Kuerbis and Mueller 2011). Similarly, while the USG's CSRIC endorsed a single root for the RPKI system, its final report noted that "since the routing system has no central authority…any viable [routing] security solution must preserve the local autonomy of these networks" (CSRIC 2012).

In summary, routing provides a clear example of networked governance. Effective global cooperation is founded on voluntary, open standards that enable network operators to exchange the information required to move packets from origin to destination automatically and rapidly. Both the basic acts of coordinating routing and the security practices intended to filter out mistaken or malicious routing information have, until now, relied almost entirely on nonhierarchical forms of governance. In the name of greater security, however, steps have been taken to introduce an element of hierarchy into this system: the RPKI. Although routed in US government-funded research, the more hierarchical system would not be administered directly by states. Additionally, the effort has met resistance because it would dramatically affect power relations among actors in the industry and its governance institutions. The US government has recognized these concerns and has not acted to overrule them. States are adapting to networked governance, not overriding it.

Incident Response: The Conficker Worm

No Internet security incident has raised the question of the scalability of the networked approach more assertively than the so-called Conficker botnet. In late 2008, a malware exploited a critical vulnerability of the Microsoft Windows operating system, installed itself in a hidden section of the operating system, and propagated rapidly and silently to millions of other machines. Infected computers thereby became part of a botnet that progressively increased in scale. The botnet and its underlying malware used a remarkably large number of known and innovative features to propagate itself, receive updates in a command-and-control structure, and make the botnet resilient against rival criminals and security countermeasures. Despite its unusual size, the botnet has only been used in a few minor cyber-crime cases, making its underlying purpose mysterious to this day.[6]

Usually, botnets are used as the infrastructure for an underground online economy. Owners of botnets, known as bot-herders, usually rent parts of them out to other criminals who then use the computer power of the botnet to send out spam or to extort Web companies by threatening distributed denial of service (DDoS) attacks. The size of the botnet can at times provide clues to the intentions and nature of the bot-herders. Next to the aforementioned use as a platform for cyber-crime, a botnet could also be used to execute DDoS attacks against government networks or other critical infrastructures, either immediately

[6]For more thorough descriptions of technical details of the Conficker botnet, cf. Microsoft (2009), Symantec (2009). Organizational issues are touched on by a DHS commissioned report (Rendon Group 2011) and a review by ICANN staff member Dave Piscitello (2010); for a journalistic narrative, cf. Bowden (2010, 2011).

or as a platform in readiness for a future attack. Even though the Conficker botnet is somewhat contained and has actually done little damage, its technical sophistication and potential for damage has awed both the technical community and (later) policymakers.

The Conficker botnet is noteworthy not only because of its impressive technical features for malware propagation and its defenses against law enforcement agencies or competing criminals, but possibly even more for its hacking of the existing incident response institutions. One fundamental anti-botnet strategy is to disinfect PCs and harden noninfected PCs by applying security patches provided by software vendors or installing new signature files from security service providers. In the case of the Stormbot botnet in 2008, for example, the issuance of a software update by Microsoft helped to solve the crisis (Keizer 2008). The second approach is to hinder botnet nodes from contacting their command-and-control servers, which are used by bot-herders to issue instructions to the bots. These approaches usually require collaboration among several actors that own or control parts of the Internet's technical infrastructure, such as anti-virus or security software vendors, domain name registrars, or Internet service providers. But special features of the Conficker worm, especially its sophisticated, automated domain name registrations, required an unprecedentedly networked response to stop its contagion.

New malware usually shows up in the so-called honeypots, deliberately weakly secured machines with a direct Internet connection designed to attract the malware that is floating around the Internet. When a malware is collected and categorized as dangerous or widespread, researchers in academia, research institutions, anti-virus and other security companies start to analyze its functionality and, if necessary, reverse engineer its entrails to provide updates for their software and anti-virus signature files. When this was done to the Conficker worm, its potentially dangerous characteristics and the large number of infected machines forced all actors involved into an unprecedented degree of collaboration. The only viable counterstrategy was to buy up hundreds of second-level domains per day, scattered over more than a hundred top-level domains. On one of these domains, the bot-herder was expected to install a command-and-control system that would tell the bots what to do next. In order to preempt the usage of the bots by the bot-herder, all the thousands of potential domains had to be registered—an endeavor for which no organizational and monetary capabilities existed. Individual interests joined forces, both for self-serving purposes and for altruistic motives to secure the Internet as a technical infrastructure from the damages that the botnet might inflict on it.

A virtual organization called the Conficker Working Group (CWG) was the umbrella for the incident response. The group was driven by individuals who either happened to be responsible for some parts of the Internet due to their professional roles (with their superiors more or less backing their detour to large-scale incident response), or voluntarily contributed their time independently of their occupational duties and roles (Schmidt 2012). But the contribution of traditional security provisioning organizations, such as law enforcement agencies, intelligence agencies, military forces, and even national Computer Emergency Response Teams (CERTs), was negligible. The containment of the threat was provided by a loose coalition of voluntary employees, entrepreneurs, and individuals. None of the actors that mattered were contractually or legally obliged to contribute to the overall response effort.

To be able to cope with the incident and to contain the Conficker threat, the organizations and individuals involved had to pool their resources in a virtual *ad hoc* organization that included individuals from the owners of major elements of the Internet. The actual shape of the *ad hoc* organization, the networked effort, and the composition of staff were predominantly contingent upon and driven by

the individuals themselves, who happened to know, get introduced to, or run into each other before or in the course of the events. Resource-wise, the only indispensable actors involved were the operators of more than one hundred top-level domain registries worldwide, as they operated those elements of the infrastructure crucial to the technical-organizational response strategy. In the response network itself, however, they only held a second-tier role in the network and by and large acted as instructed by the CWG core team and ICANN.

At the same time, the institutional design of the response effort was rooted in earlier policy decisions forbearing from more direct regulation. Governments in Western and democratic countries had liberalized both basic telecommunications infrastructure and the supply of software, equipment, and technical standards. Most of the information services running over that infrastructure had been largely deregulated. Divergent as the private actors' interests were, they shared an interest in the technical well-being of the Internet. Hence, particular private interests joined forces to provide a public good. In a sense, the *ad hoc* response organization was a just-in-time response of the industry and Internet bodies to the emerging problem of large-scale botnets. Hence, to some extent, self-governance of the industry worked. And so did modern management approaches that prescribe bottom-up initiative that reach out to external organizations in rapidly changing environments with many unknown risks. The community of technical experts managed to respond organizationally to the botherders' hack and their exploitation of DNS and security industry vulnerabilities.

The Conficker response effort, though, raises questions about the scalability of global Internet incident response. It is possible that an attacker could exploit technical and organizational vulnerabilities on an increased scale and/or with increasing frequency, requiring even more intense global collaboration among a greater number of actors. Add another acute cyber incident, and the anti-Conficker security provisioning model might reach a state of overextension. Some response activities require manual, repetitive, meticulously executed interventions. However, a lot of the contributions to these voluntary collaborative communities are motivated by an interest in solving new, challenging technological problems (Lakhani and Wolf 2003). Repetitive tasks crowd out the "*homo ludens* payoff" (Bitzer, Schrettl, and Schröder 2007:168). Therefore, some kind of institutionalization of the response organization may be necessary in the future.

Aside from these global public policy dimensions, the problem of Internet security touches on the focal point of authority and its ability to unilaterally enforce policy goals—and thereby on classic questions in IR studies. The Conficker botnet continues to exist, albeit on a smaller scale compared to its peak time, posing a potential threat (Microsoft 2012). Remediation would require the removal of malware from infected machines and updating insecure systems. But this would require technical control over individual machines, which resides with their respective owners. There are no means at hand to coerce users of infected machines scattered all over the world, mainly in BRIC countries,[7] to upgrade their machines. Therefore, short-term remediation of Conficker appears to be only achievable by acts of benevolent hacking; that is, by exploiting known weaknesses of the malware or of infected machines to get it removed without the owners' consent or knowledge (Leder, Werner, and Martini 2009). The potential legal, economic, and political repercussions of such unauthorized actions mean that both public and private actors are hesitant to engage in such hacking. The sole exception so far has been the Bredolab case, in which the Dutch police used confiscated command-and-control systems to make the bots download a software that would support users in cleaning their infected systems (Schlösser

[7]Cf. Shadowserver Foundation, "Conficker Statistics," http://www.shadowserver.org/wiki/pmwiki.php/Stats/Conficker.

2011:17). Whether sponsored by states or corporations, such intrusions could have tremendous implications for the privacy and personal integrity of Internet users. On the international scale, benevolent hacking would potentially include machines owned by government organizations in BRIC countries, and might be perceived as a politically threatening act in these countries.

In the long run, future operating systems and software update mechanisms might allow vendors to force-update their installed base, just as Google can already remotely uninstall applications from Android devices (von Eitzen 2010). These forced remote-sanitizing tactics might be one of the capabilities built up in offensive cyber-warfare squadrons, and only applied if a botnet is eventually turned into an attack platform to take down critical infrastructures. But if rival states began to compete over the creation and use of these capabilities, that could become a security threat as much as a security solution.

Discussions within the CWG raised yet another aspect of international politics and revealed how independent, bottom-up initiatives can still favor one billiard ball over others in the classic game of international politics. Within the group, disagreement arose as to how to secure the cooperation of the Chinese top-level domain operator and whether to share information with China about infected machines. Sharing the IP addresses of infected machines would have given untrusted parties insights into the networks of owned organizations and, in combination with knowledge about the vulnerabilities of the Conficker malware itself, clues how to compromise these networks. From a policing and apolitical technological perspective, such widespread sharing makes perfect sense. If, however, one assumes that the botnet might be intended to serve as a state-sponsored DDoS-attack platform and that knowledge of vulnerable machines is of interest to state-sponsored intelligence services, then any such sharing might level out informational advantages among states. Experts involved in the response effort were partly contractually prohibited from sharing such insights.

While Internet security has the characteristics of a public good in some situations, the ingredients necessary to create it certainly are not. The response team was almost exclusively based in the United States and appears to have followed US-centered security considerations. In this regard, the response team was more akin to a US-based club than a neutral global community of technically interested experts.

Concluding Observations

The preceding section provided two moderately detailed analyses of security production on the Internet. Routing and botnet mitigation are not arbitrary or cherry-picked cases. Routing is a form of coordination fundamental to Internet operations, and protecting it from manipulation or attack is a major preoccupation of the Internet standards and operations communities at this time. Botnets are widely recognized as one of the chief plagues of the Internet,[8] providing an infrastructure for spam, cyber-crime, and DDoS attacks, and the Conficker botnet was unusual in its scope and scale. It is significant, therefore, to see a heavy reliance on networked governance in both cases, and the effectiveness of the coordination and mitigation so achieved.

The attempt to introduce more hierarchical authority into routing, while aided by US government-funded research and supported by some recent coordinative efforts by the US FCC, still proposes to rely on private actors and private-

[8]The nonprofit Shadowserver Foundation estimates that there currently some 2,200 active command-and-control servers, although some botnets have more than one C&C server (http://www.shadowserver.org/wiki/pmwiki.php/Stats/BotnetCharts). Security company Damballa counted 872 botnets with more than one hundred bots. Of these 872 botnets, 5 control more than 1 million bots and 37 more than 100,000 (Damballa 2011).

sector-based governance entities to create and maintain the hierarchy. In order to create a globally effective locus of hierarchical authority, the advocates of RPKI have proposed to use either ICANN, the RIRs, or some combination of both as trust anchors for certificates—*not* the world's national governments or intergovernmental organizations. The reason for this is clear: In many respects, the attempt to secure routing via a hierarchical PKI infrastructure reproduces the dreaded problem of the single root that has made the politics of ICANN so fraught with geopolitical tension (Mueller 2002; Klein 2002; Crampton 2005). Insofar as the top of the hierarchy is seen as being under the control of a single nation-state, the security mechanism becomes unacceptable to rival nation-states. But a hierarchical mechanism that involves the participation and agreement of all nation-states would probably take years to negotiate because of those same political differences and may also become ensnared in nationally backed competing technologies or incompatible standards of the sort described by Drezner (2007). It should also be noted that states or state-backed actors pursuing geopolitical, military, or surveillance goals could undermine the integrity of PKI certificates. Thus, bringing states in as the preeminent actor in ensuring routing security not only raises political impediments to adoption, but does not necessarily create more security.

If there is a single root, someone must stand at the top of the hierarchy. No matter where one proposes to delegate that authority—to a single private-sector entity such as ICANN, to a single government or small club of governments, or to an intergovernmental treaty organization—deciding who will hold that role is not simple, nor does it guarantee security for anyone except the supreme hierarch. In the RPKI proposal, entities lower in the proposed hierarchy, especially the network operators, did not embrace the new approach because of the loss of autonomy it would involve. Thus, implementing a hierarchical regime that is truly global and effective raises profound issues of power, institutional design, and legitimacy. Short of that, trust anchor adoption by operators is likely to be based more on a network model of trust, with multiple alternative trust anchors and even competing national certificate authorities. And that leads us right back into networked governance of routing.

The Conficker case exemplified a collaborative network of volunteering technical experts who joined forces *ad hoc* to provide public Internet security. We did not see the limited, networked "Lego state" of Slaughter at work; instead, state authorities were effectively absent in the response. The role of the state was similarly minor in a previous Internet security incident, the Estonian cyber attacks in 2007, where stark policy rhetoric from NATO allies did not alter the basic fact that states contributed practically nothing to mitigating the technical situation (Schmidt 2013).

But in both cases we see states attaching themselves to these networks of operators and technical experts and (in the case of the United States) directly influencing the standardization process. The technical community itself has asked the state to prosecute bot-herders, which a mere technical approach cannot do. While the Conficker case in isolation seems to indicate that the state's authority over communication and information is being hollowed out by the rise of the Internet, subsequent anti-botnet activities responding to the DNS Changer scam (von Eitzen 2011), the BredoLab botnet (Schwartz 2010), the Mariposa botnet (Sully and Thompson 2010; Kolakowski 2010), and the ZeuS botnets (Lennon 2012) involved governmental law enforcement agencies from different nations working extensively with the private-sector actors. In all these cases, transnational law enforcement had a significantly more prominent role than in the Conficker response, showing that state authorities are embedding themselves into existing technical-operational networks. In addition to these multistakeholder alliances, studies of the London Action Plan, a textbook TGN

involving government agencies and some private corporations in anti-spam efforts, also reveal effective network organization (Tabatabaie, van Eeten, and Asghari 2012). These phenomena align with a general trend in policing toward greater reliance on private actors (Kempa, Carrier, Wood, and Shearing 1999; Krahmann 2005).

Thus, networked collaboration is likely to persist, albeit with increased collaboration between operators and law enforcement agencies. Rather than a strict imposition of hierarchy, we see greater networked collaboration. Indeed, it is difficult to imagine circumstances in which all states would agree on a common global "botnet authority" given geopolitical rivalries and differing national interests. More likely, we will see conflicts about positions within these networks, and attempts by actors to favorably position themselves and to set the agenda and the norms within these networks. In those few botnet takedowns so far, we have seen in one case police forces dominating the response activities (Bredolab), in other cases a software vendor like Microsoft taking the lead (ZeuS, Waledac, Rustock botnets) and at other times an ad hoc group of security experts, security vendors, software vendors, law enforcement, academics, and others (Conficker, Mariposa).

The case studies thus show the state as just one player among others and reveal the inability of states or transnational security organizations to act as the monopoly of force enforcing preferred cyberspatial outcomes. Our conclusion, therefore, runs counter to recent policy trends emerging from the national security and foreign policy community, which still nurture the hypothesis that, in the name of cyber-security, states can or should build up contingency capabilities such as an Internet "kill switch," far-reaching surveillance and identification capabilities, and the equation of cyber attack with a traditional physical force attack (Pear 2012; McConnell 2010; Gorman and Barnes 2011).

As the Internet is portrayed in many policy debates as a source of threats to national security interests, states can be expected to establish robust coercive means and contingency capabilities. But such attempts, to be globally effective, would require altering technical standards and/or operational practices to allow for the full exercise of hierarchical authority. Any attempts by states to do this faces huge challenges. *De facto* control over the Internet's technical components and the data flowing through them is exercised by private actors; these actors are located in different countries and are supported by a global community of technical experts and open standards. Their contributions are indispensable to efforts to handle common Internet security issues, and their motivation to contribute is beyond a single state's reach. A second challenge to unilateral national attempts to increase security is their potentially detrimental effects on Internet security. No group of states is likely to acquiesce in hierarchical arrangements that elevate another state. Attempts by states to fundamentally alter the existing distribution of power in security provisioning networks are likely to lead to decreased performance of these networks and consequently a deteriorated Internet security situation. The extreme transnational interdependence in Internet operations require globalized institutions to be effective.

To conclude with answers to our research questions: First, networked governance on the Internet is not necessarily incompatible with states' security concerns. Networked forms of organization can and do develop methods of cooperating to handle Internet security, and states have played a role in such collaborations. But such methods do seem to be incompatible with traditional notions of territorial sovereignty and the close alignment of communications infrastructures with national entities. Second, states are adapting to networked governance not by asserting direct, hierarchical control over it, but by inserting themselves into the technical and operational networks and attempting to shape standards and practices in a multistakeholder environment. Both cases analyzed

in this paper raised doubts about the claim that introducing security concerns into Internet governance necessarily leads to more hierarchy and/or a greater role for national governments.

Networked organizational forms thus need to be better understood and taken more seriously as the basis for Internet governance. It is important to recognize both their historic contribution to growth and innovation in transnational communications, and their resilience in meeting current challenges. While they may have flaws and breakdowns occasionally, attempts to move toward more hierarchical organizational forms will not be easy and are likely to generate conflicts and problems of their own, particularly if the hierarchy involves contending states.

References

Adler, Paul S. (2001) Market, Hierarchy, and Trust: The Knowledge Economy and the Future of Capitalism. *Organization Science* 12 (2): 215–234.

Bates, T., E. Gerich, L. Joncheray, J.-M. Jouanigot, D. Karrenberg, M. Terpstra, and J. Yu. (1995) Representation of IP Routing Policies in a Routing Registry (ripe-81 + +) RFC 1786. IETF.

Benkler, Yokai. (2006) *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven: Yale University Press.

Bitzer, Jürgen, Woldfram Schrettl, and Philipp Schröder. (2007) Intrinsic Motivation in Open Source Software Development. *Journal of Comparative Economics*, 35 (1): 160–169.

Boerzel, Tanja A. (1998) Organizing Babylon—On the Different Conceptions of Policy Networks. *Public Administration* 36 (1): 3–18.

Bowden, Mark. (2010) The Enemy Within. The Atlantic (June). Available at http://www.theatlantic.com/magazine/archive/2010/06/the-enemy-within/8098/1/. (Accessed October 2, 2012.)

Bowden, Mark. (2011) *Worm—The First Digital World War*. New York: Atlantic Monthly Press.

Bryden, Alan, and Marina Caparini. (2006) *Private Actors and Security Governance*. Münster: Lit Verlag.

Butler, Kevin, Toni R. Farley, Patrick McDaniel, and Jennifer Rexford. (2010) A Survey of BGP Security Issues and Solutions. *Proceedings of the IEEE* 98: 100–122.

Clark, David D., and Susan Landau. (2011) Untangling Attribution. *Harvard National Security Journal* 2 (2): 531–562.

Coase, Ronald H. (1937) The Nature of the Firm. *Economica* 4: 386–405.

Coase, Ronald H. (1960) The Problem of Social Cost. *Journal of Law and Economics* 3 (1): 1–44.

Communications Security, Reliability and Interoperability Council III (CSRIC). (March 2012) Secure BGP Deployment. Report. Working Group 6: Secure BGP Deployment. Report. Available at http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG6-Final-Report.pdf. (Accessed October 2, 2012.)

Cowhey, Peter, and Milton Mueller. (2009) Delegation, Networks and Internet Governance. In *Networked Politics: Agency, Power and Governance*, edited by Miles Kahler. Ithaca, NY: Cornell University Press.

Crampton, Thomas. (2005) "The 'Root Zone' of a Web Dispute." *New York Times*: Technology, September 30, 2005. Available at http://www.nytimes.com/2005/09/30/technology/30iht-web.html. (Accessed October 2, 2012.)

Damballa, Labs. (2011) Threat Report. First Half 2011. Atlanta: Damballa Inc. Available at https://www.damballa.com/downloads/r_pubs/Damballa_Threat_Report-First_Half_2011.pdf. (Accessed October 2, 2012.)

Dean, Jodi, Jon W. Anderson, and Geert Lovink, Eds. (2006) *Reformatting Politics: Information Technology and Global Civil Society*. London: Routledge.

Deibert, Ronald J., and Masashi Crete-Nishihata. (forthcoming) Global Governance and the Spread of Cyberspace Controls. *Global Governance* 18: 339–361.

Dorussen, Han, and Hugh Ward. (2008) Intergovernmental Organizations and the Kantian Peace: A Network Perspective. *Journal of Conflict Resolution* 52 (2), April: 189–212.

Drezner, Daniel. (2007) *All Politics Is Global: Understanding International Regulatory Regimes*. Princeton: Princeton University Press.

Dunn Cavelty, Myriam. (2008) *Cyber-Security and Threat Politics*. London, New York: Routledge.

Dunn Cavelty, Myriam. (2013) From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review* 15(1): 105–122.

Economides, Nicholas. (1996) The Economics of Networks. *International Journal of Industrial Organization* 14 (6), October: 673–699.

Eilstrup-Sangiovanni, Mette. (2009) Varieties of Cooperation: Government Networks in International Security. In *Networked Politics: Agency, Structure and Power*, edited by Miles Kahler. Ithaca, NY: Cornell University Press.

von Eitzen, Christopher. (2010) Google Uses Remote Delete to Remove Android Apps from Smartphones. The H Security. June 25. Available at http://www.h-online.com/security/news/item/Google-uses-remote-delete-to-remove-Android-apps-from-smartphones-Update-1029188.html. (Accessed October 2, 2012.)

von Eitzen, Christopher. (2011) Operation Ghost Click: FBI Busts DNSChanger botnet. The H Security. November 10. Available at http://www.h-online.com/security/news/item/Operation-Ghost-Click-FBI-busts-DNSChanger-botnet-1376746.html. (Accessed October 2, 2012.)

ENISA. (2010) Report on Secure Routing Technologies. Crete, Greece, European Network and Information Security Agency and Institute of Communications and Computer Systems (ICCS)

Fung, Archon, Hollie Russon Gilman, and Jennifer Shkabatur. (2013) Six Models for the Internet + Politics. *International Studies Review* 15(1): 30–47.

George, Alexander L., and Andrew Bennett. 2005. *Case Studies and Theory Development in the Social Sciences*. BCSIA Studies in International Security. Cambridge, MA: MIT Press.

Gorman, Siobhan, and Julian E. Barnes. (2011) Cyber Combat Can Count as Act of War. *Wallstreet Journal* Available at http://professional.wsj.com/article/SB10001424052702304563104576355623135782718.htm. (Accessed October 2, 2012.)

Granovetter, Mark. (1985) Economic Action and Social Structure: The Problem of Embeddedness. *American Journal of Sociology* 91 (3): 481–510.

Hafner-Burton, Emilie, Miles Kahler, and Alexander H. Montgomery. (2009) Network Analysis for International Relations. *International Organization* 63 (3): 559–592.

Howard, Philip N. (2006) *New Media Campaigns and the Managed Citizen*. Cambridge: Cambridge University Press.

Huston, Geoff. (2009) Resource Certification. *IETF Journal*, 4 (3): 21–28.

Jones, Candace, William S. Hesterly, and Stephen P. Borgatti. (1997) A General Theory of Network Governance: Exchange Conditions and Social Mechanisms. *Academy of Management Review* 22 (4): 911–945.

Kahler, Miles, Ed. (2009) *Networked Politics: Agency, Structure and Power*. Ithaca, NY: Cornell University Press.

Keizer, Gregg. (2008) Microsoft: We Took Out Storm Botnet. eWeek, April 22. Available at http://www.computerworld.com/s/article/9079653/Microsoft_We_took_out_Storm_botnet. (Accessed October 2, 2012.)

Kempa, Michael, Ryan Carrier, Jennifer Wood, and Clifford Shearing. (1999) Reflections of the Evolving Concept of "Private Policing." *European Journal on Criminal Policy and Research* 7 (2): 197–223.

Kent, Stephen. (2006) An Infrastructure Supporting Secure Internet Routing. In *Public Key Infrastructure: Third European PKI Workshop*, edited by Antonio S. Atzeni and Andrea Lioy. Berlin, Heidelberg: Springer.

Kent, Stephen, Charles, Lynn, and Karen, Seo. (2000) Secure Border Gateway Protocol (S-BGP). *IEEE Journal on Selected Areas in Communications* 18 (4): 582–592, April

Klein, Hans. (2002) ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy. *The Information Society* 18: 193–207.

Knox, Hannah, Mike Savage, and Penny Harvey. (2006) Social Networks and the Study of Relations: Networks as Method, Metaphor and Form. *Economy and Society* 35 (1): 113–140.

Kolakowski, Nicholas. (2010) Spain, IT Security Companies Sting Mariposa Botnet. eWeek, March 3. Available at http://www.eweek.com/c/a/Security/Spain-IT-Security-Companies-Sting-Mariposa-Botnet-390027/. (Accessed October 2, 2012.)

Kooiman, Jan. (2003) *Governing and Governance*. London: Sage.

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

Krahmann, Elke. (2010) *States, Citizens and the Privatization of Security*. Cambridge, UK, New York: Cambridge University Press.

Kuerbis, Brenden, and Milton Mueller. (2011) Negotiating a New Governance Hierarchy: An Analysis of the Conflicting Incentives to Secure Internet Routing. *Communications and Strategies* 81, First Quarter: 125–142.

Labovitz, Craig. (2010) China Hijacks 15% of Internet Traffic? Arbor Networks Security to the Core blog, November 19, 2010. Available at http://asert.arbornetworks.com/2010/11/china-hijacks-15-of-internet-traffic. (Accessed October 2, 2012.)

Lakhani, Karim R., and Robert G. Wolf. (2003) Why Hackers Do what They Do: Understanding Motivation and Effort in Free/Open Source Software Projects. *SSRN ELibrary* doi:10.2139/ssrn.44304.

Leder, Felix, Tillmann Werner, and Peter Martini. (2009) Proactive Botnet Countermeasures—An Offensive Approach. In *The Virtual Battlefield: Perspectives on Cyber Warfare. The Proceedings of the Conference on Cyber Warfare 2009*, edited by Kenneth Geers and Christian Czosseck. Tallinn: CCD COE Publications & IOS Press. Available at http://www.ccdcoe.org/230.html. (Accessed June, 2010.)

Lennon, Mike. (March 26, 2012) Microsoft Leads Sting Operation to Disrupt Zeus Botnets. SecurityWeek. Available at http://www.securityweek.com/microsoft-and-partners-disrupt-zeus-botnets-sting-operation. (Accessed October 2, 2012.)

Maoz, Zeev, Lesley G. Terris, Ranan D. Kuperman, and Ilan Talmund. (2003) International Relations: A Network Approach. Gilman Conference on new directions in international relations. Yale University. Available at http://soc.haifa.ac.il/~talmud/pdf/irnetworks1.pdf. (Accessed October 2, 2012.)

McConnell, Mike. (2010) Mike McConnell on How to Win the Cyber-war We're Losing. *Washington Post*, Opinions, February 28. Available at http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html. (Accessed October 4, 2012.)

Microsoft. (2009) Microsoft Security Intelligence Report, January through June, 2009. November 2009. Vol. 7. Available at http://www.microsoft.com/sir. (Accessed October 2, 2012.)

Microsoft. (2012) Microsoft Security Intelligence Report, July through December, 2011. Vol. 12. Available at http://www.microsoft.com/sir. (Accessed October 2, 2012.)

Mueller, Milton L. (2002) *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge, MA: MIT Press.

Mueller, Milton L. (2010) *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: MIT Press.

Nye, Joseph S. (2011) Nuclear Lessons for Cybersecurity? *Strategic Studies Quarterly* (Winter) 18–38.

Ohanyan, Anna. (2009) Policy Wars for Peace: Network Model of NGO Behavior. *International Studies Review* 11/3 (September): 475–501.

Pear, Robert. (2012) House Votes to Approve Disputed Hacking Bill. *New York Times*. April 26. Available at http://www.nytimes.com/2012/04/27/us/politics/house-defies-veto-threat-on-hacking-bill.html?_r=1andref=technology. (Accessed October 2, 2012)

Piscitello, Dave. (2010) Conficker Summary and Review. ICANN. Available at https://www.icann.org/en/security/conficker-summary-review-07may10-en.pdf. (Accessed October 2, 2012.)

Powell, Walter W. (1990) Neither Market nor Hierarchy: Network Forms of Organization. *Research in Organizational Behavior* 12: 295–336.

Raustiala, Kal. (2002) The Architecture of International Cooperation: Transgovernmental Networks and the Future of International Law. *Virginia Journal of International Law* 43: 1–92.

Reinicke, Wolfgang H. (1997) Global Public Policy. *Foreign Affairs* 76 (6): 127–139.

Rendon Group. (2011) Conficker Working Group: Lessons learned. January. (Report created in June 2010, commissioned by the Department of Homeland Security) Available at http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf. (Accessed October 2, 2012.)

Rohlfs, Jeffrey. (1974) A Theory of Interdependent Demand for a Communications Service. *Bell Journal of Economics* 5 (1): 16–37.

Scharpf, Fritz W., Ed. (1993) *Games in Hierarchies and Networks: Analytical and Empirical Approaches to the Study of Governance Institutions*. Frankfurt and Boulder: Campus Verlag and Westview Press.

Scharpf, Fritz W. (1997) *Games Real Actors Play: Actor-centered Institutionalism in Policy Research*. Boulder: Westview Press.

Schlösser, Mark. (2011) Computerviren, Malware, Botnetze - Dürfen wir uns wehren. Presentation given at the RWTH Wissenschaftsnacht, November 11, Aachen. Website of IT Security Research Group, RWTH Aachen University. Available at http://itsec.rwth-aachen.de/people/rwth_wnacht_malware_mschloesser_111111.pdf. (Accessed October 2, 2012.)

Schmidt, Andreas. (2012) At the Boundaries of Peer Production: The Organization of Internet Security Production in the Cases of Estonia 2007 and Conficker. *Telecommunications Policy* 36 (6): 451–461.

Schmidt, Andreas. (Forthcoming). The Estonian Cyberattacks. In *The Fierce Domain: Conflict in Cyberspace 1986 -2012*, edited by Jason Healey. Washington, DC: Atlantic Council.

Schneider, Volker, and Raimund Werle (1991) Policy Networks in the German Telecomunications Domain. In *Policy Networks: Empirical Evidence and Theoretical Considerations*, edited by Bernd Marin and Renate Mayntz. Boulder: Westview Press.

Schwartz, Mathew J. (2010) Bredolab Botnet Busted. InformationWeek. October 27. Available at http://www.informationweek.com/story/showArticle.jhtml?articleID=22800009. (Accessed October 2, 2012.)

Seo, Karen, Charles Lynn, and Stephen Kent. (2001) Public-key Infrastructure for the Secure Border Gateway Protocol (S-BGP). Proceedings of DARPA Information Survivability Conference and Exposition II (DISCEX'01), Anaheim, California, IEEE Computer Society.

Siganos, Georgos, and Michalis, Faloutsos. (2004) Analyzing BGP Policies: Methodology and Tool. *Proceedings IEEE INFOCOM 2004, 23rd Annual Joint Conference of the IEEE Computer and Communications Societies*. New York: IEEE; 1640–1651.

Siganos, Georgos, and Michalis, Faloutsos. (2007) Neighborhood Watch for Internet Routing: Can We Improve the Robustness of Internet Routing Today?. *IEEE INFOCOM 2007, 26th IEEE International Conference on Computer Communications*. New York: IEEE; 1271–1279.

Singh, J.P. (2013) Information Technologies, Meta-power, and Transformations in Global Politics. *International Studies Review* 15(1): 5–29.

Slaughter, Anne-Marie. (1997) The Real New World Order: The State Strikes Back. *Foreign Affairs* 76 (5): 183–197.

Slaughter, Anne-Marie. (2004) *A New World Order*. Princeton, NJ: Princeton University Press.

Sørenson, Eva, and Jacob Torfing. (2007) *Theories of Democratic Network Governance*. Basingstoke: Palgrave McMillan.

Sriram, Kotikapaludi, Oliver Borchert, Okhee Kim, Patrick Gleichmann, and Doug Montgomery. (2009) A Comparative Analysis of BGP Anomaly Detection and Robustness Algorithms. *2009 Cybersecurity Applications & Technology Conference for Homeland Security*. New York: IEEE; 25–38.

Sully, Matt, and Matt Thompson. (2010) The Deconstruction of the Mariposa Botnet. Defence Intelligence. Available at http://defintel.com/docs/Mariposa_White_Paper.pdf. (Accessed October 2, 2012.)

Symantec (June 2, 2009) The Downadup codex. A Comprehensive Guide to the Threat's Mechanics (2.0 ed.). Available at http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_downadup_codex_ed2.pdf. (Accessed October 2, 2012.)

Tabatabaie, Shirin, Michel van Eeten, and Hadi Asghari. (2012) Transgovernmental Networks in Cybersecurity: A Quantitative Analysis of the London Action Plan Against Spam. Paper presented at the 2012 Annual Convention of the International Studies Association.

Thompson, Grahame. (2003) *Between Hierarchies and Markets: The Logic and Limits of Network Forms of Organization*. Oxford: Oxford University Press.

Thorelli, Hans B. (1986) Networks: Between Markets and Hierarchies. *Strategic Management Journal* 7 (1): 37–51.

USCESRC (US China Economic and Security Review Commission). (2010) Report to Congress of the U.S.-China Economic and Security Review Commission. One Hundred Eleventh Congress, Second Session, November 2010.

Williamson, Oliver E. (1975) *Markets and Hierarchies, Analysis and Antitrust Implications: A Study in the Economics of Internal Organization*. New York: Free Press.

Williamson, Oliver E. (1985) *The Economic Institutions of Capitalism: Firms, Markets, Relational Contracting*. New York: Free Press.

Wong, Wendy, and David Lake. (2009) The Politics of Networks: Interests, Power, and Human Rights Norms. In *Networked Politics: Agency, Power, and Governance*, edited by Miles Kahler. Ithaca, NY: Cornell University Press.