MIT ESD

Massachusetts Institute of Technology
Engineering Systems Division

ESD Working Paper Series

Institutional Foundations for Cyber Security: Current Responses and New Challenges

Nazli Choucri
Professor of Political Science
MIT Department of Political Science
Massachusetts Institute of Technology
Email: nchoucri@mit.edu

Jeremy Ferwerda
Graduate Research Assistant
MIT Department of Political Science
Massachusetts Institute of Technology
Email: ferwerda@mit.edu

Stuart Madnick
John Norris Maguire Professor of Information Technology and Professor of Engineering Systems
MIT Sloan School of Management and MIT School of Engineering
Massachusetts Institute of Technology
Email: smadnick@mit.edu

ESD-WP-2014-33 November 2014 esd.mit.edu/wps

Institutional Foundations for Cyber Security: Current Responses and New Challenges

Nazli Choucri, Stuart Madnick, Jeremy Ferwerda

Working Paper CISL# 2013-16

October 2013

Composite Information Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

Information Technology for Development, 2013
http://dx.doi.org/10.1080/02681102.2013.836699

Institutions for Cyber Security: International Responses and Global Imperatives

Nazli Choucri[a], Stuart Madnick[b*] and Jeremy Ferwerda[a]

[a]*Department of Political Science, MIT, Cambridge, MA, USA;* [b]*Sloan School of Management, MIT, 30 Wadsworth Street, Room E53-321, Cambridge, MA 02139, USA*

Almost everyone recognizes the salience of cyberspace as a fact of daily life. Given its ubiquity, scale, and scope, cyberspace has become a fundamental feature of the world we live in and has created a new reality for almost everyone in the developed world and increasingly for people in the developing world. This paper seeks to provide an initial baseline, for representing and tracking institutional responses to a rapidly changing international landscape, real as well as virtual. We shall argue that the current institutional landscape managing security issues in the cyber domain has developed in major ways, but that it is still "under construction." We also expect institutions for cyber security to support and reinforce the contributions of information technology to the development process. We begin with (a) highlights of international *institutional theory* and an *empirical* "census" of the institutions-in-place for cyber security, and then turn to (b) key imperatives of *information technology-development linkages* and the various cyber processes that enhance developmental processes, (c) major *institutional responses to cyber threats and cyber crime* as well as select international and national policy postures so critical for industrial countries and increasingly for developing states as well, and (d) the salience of *new mechanisms* designed specifically in response to cyber threats.

Keywords: cyber security; cyber governance; cyber institutions; sustainable development; CERTs; information technology

1. Introduction

The expansion of cyberspace has occurred at a dramatic pace over the past two decades. Almost every location on the globe now has some degree of cyber access, outpacing even the most optimistic expectations of the early architects of the Internet. Less anticipated, however, by the initial innovators or anyone else, was the subsequent introduction of cyber threats and the accompanying innovations in the disruption and distortion of cyber venues.

This paper is positioned at the intersection of the long tradition of international institutions and the nascent area of theorizing about cyberpolitics in international relations. Its purpose is to provide an initial baseline, for representing and tracking institutional responses to a rapidly changing international landscape, real as well as virtual. In this paper, we shall argue that the current institutional landscape managing security issues in the cyber domain has developed in major ways, but that it is still "under construction." We also anticipate that institutions for cyber security will support and reinforce the contributions of information technology to the development process.

For purposes of context and background, we (a) begin with highlights of international *institutional theory* and an *empirical* "census" of the institutions-in-place for cyber security, and then

*Corresponding author. Email: smadnick@mit.edu
Doug Vogel is the accepting Associate Editor for this article.

turn to (b) key imperatives of *information technology-development linkages* and the various cyber processes that enhance developmental processes, (c) major *institutional responses to cyber threats and cyber crime* as well as select international and national policy postures so critical for industrial countries and increasingly for developing states as well, and (d) the salience of *new mechanisms* designed specifically in response to cyber threats.

2. International institutions: theoretical anchors and empirical record

Over the better part of a decade, the convergence of four distinct but interconnected trends in international relations created demands for formal interventions involving governments and international coordination. First, Internet usage continued to rise, coupled with an expansion in forms of use. Second, many governments recognized that cyber vulnerabilities continued to threaten not only the security of their own networks, but also those of their citizens involved in routine activities on a daily basis. Third, a noted absence of coordinated industry response or of efforts to develop cooperative threat reduction strategies, reinforced an unambiguous gap-in-governance. Finally, a growing set of cyber incidents, large and small, signaled to governments the potential impact of their failure to address the emerging threats. In response to these trends, governments, in various ways, mobilized significant national and international resources toward the creation of a broad cyber security framework.

2.1 *Theoretical context*

There is a long, respected, and distinguished tradition of institution-centric scholarship in modern international relations. The classical literature in this field focused on the United Nations (UN) and its institutions against a background of the failures of the League of Nations;[1] this literature was largely descriptive, highlighting structure and function.[2] With the evolution of European integration, institutionalism took a new turn, seeking to connect domestic and international politics and to signal potentials for diffusion of institutional development.[3] Subsequently, the conceptual frame of reference shifted to focus on "demand" and "supply" driving the development of international institutions.[4]

Subsequently, the concept of *regime* emerged as an important anchor in the field. In this paper, however, we focus on the formal aspects of regimes, namely the institutional manifestations, rather than on underlying norms and principles. In a review of institutionalism theory, Hall and Taylor (1996) argue that contemporary institutionalism, known as "new institutionalism," is actually an amalgam of three types of theoretical considerations rather than one single theory – namely historical institutionalism, rational choice institutionalism, and sociological institutionalism. The first focuses largely on constitutional issues, bureaucratic arrangements, and operating procedures of interaction. The second, rational choice institutionalism, centers on the value of reduced transaction costs, the relationship between principals and agents, and strategic interaction – all based on the underlying logic of rational choice. Sociological institutionalism, the third variant, concentrates largely on why organizations adopt particular sets of institutional forms, including procedures and symbols.

A somewhat different perspective on institutional issues in the context of the sovereign state, put forth by Reich (2000), argues that the relevant institutional features or theoretical perspectives should be viewed in the context of the specific case in question. This view is based on Lowi (1964), who argued that the policy domains, or subject matter, dictate the "best" institutional forms – thus placing the empirical context in the forefront and matters of theory in a derivative position. This pragmatic perspective fits well with the policy imperatives created by the cyber domain.

While the literature tends to argue that consensus on norms precedes the formation of institution, we suspect that in the cyber domain the reverse dynamics hold, namely that institutions may well be the precursors for formalizing norms and principles that, in turn, might consolidate and strengthen the institutions themselves. This contingency is especially likely in the development context.

2.2 *Institutional "ecosystem": a baseline*

Building a "baseline" for cyber security institutions in international relations is particularly daunting given the trajectory of evolution for the cyber domain.

To begin with, cyberspace was constructed by the private sector – albeit with the support and direction of the dominant power in world politics, the USA. The state system formally defined in cyberspace is a relatively recent development; the entire cyber domain is managed by non-state entities, an important aspect of scale and scope in international relations.

Second, the usual mechanisms for tracking activities in the physical world – statistics, standards, measurements, etc. – are not automatically conducive to "virtual" traces or counterparts.

Third, the very nature of the "virtual" contradicts that which is physical. Threats in the "virtual" domain are often identified after the fact, rather than tracked "in process." In the cyber domain, there is not only no early warning system, there are as yet few early signals of a cyber threat, if any.

The broad institutional domain presented in Table 1 provides a baseline view of the cyber security "institutional ecosystem" which is a complex assortment of national, international, and private organizations. Parallel to the organic fashion in which cyberspace itself developed, these organizations often have unclear mandates or possess overlapping spheres of influence. Our purpose here is only to highlight these major entities and, to the extent possible, to signal their relationships and interconnections, compiling something of a census of institutions. A secondary, but also important, objective is to explore data quality and the extent to which we may infer organizational performance from public metrics, creating a performance assessment of sorts.

While we catalogue many of the major institutional players in this aspect of cyber security, we do not claim to provide an exhaustive "census." We used two criteria for the selection of institutions, namely (a) *data provision* of public qualitative or quantitative data in each of our areas of focus (international, intergovernmental, national, non-profit, and private sector) and (b) *coordination responsibility* based on formal mandates issued by recognized international or national bodies. For the national sphere, we focused on the USA as a representative model but also included several examples of non-US national entities; detailed analysis of other national efforts is beyond the scope of this paper.

3. Information technology and development linkages

The academic as well as the policy communities worldwide have long focused on challenges associated with economic, social, and political development, broadly defined. Throughout the entire immediate World War II period, the decolonization process created a whole new "generation" of governments whose vision of governance required adaptation to the new challenges, and whose limited capability required immediate enhancement if any possibility of effective performance is to be realized.

The development agenda of the international community recognized the complexity of the foregoing, and over time the requisite institutional mechanisms were put in place. Some were

Table 1. International institutional ecosystem.

Institution	Role	Data availability	Example variables (if applicable)
CERTs			
AP-CERT	Asian regional coordination	High	Collation of security metrics from member CERTs in Asia
CERT/CC	Coordination of global CERTs, especially national CERTs.	Moderate	Vulnerabilities catalogued, hotline calls received, advisories and alerts published, incidents handled
FIRST	Forum and information sharing for CERTs	Low	Secondary data from conferences and presented papers
National CERTS (e.g. US-CERT)	National coordination; national defense and response	High	Varies – volume of malicious code and viruses, vulnerability alerts, botnets, incident reports
TF-CSIRT: Computer Security Incident Response Teams	European regional coordination	N/A	N/A
International entities			
CCDCOE	Enhancing NATO's cyber defense capability	N/A	N/A
Council of Europe	International legislation	Moderate	Legislation and ratification statistics; secondary data from conferences and presented papers.
EU: European Union	Sponsors working parties, action plans, guidelines	N/A	N/A
ENISA	Awareness-raising, cooperation between the public and private sectors, advising the EU on cyber security issues, data collection	Low	Awareness-raising stats, spam surveys, regional surveys, country reports. Qualitative data assessing the EU cyber security sphere
G8: Subgroup on High-Tech Crime	Sponsored 24/7 INTERPOL hotline, various policy guidelines	N/A	N/A
IMPACT	Global threat response center, data analysis, real-time early warning system	N/A[a]	N/A[a]
INTERPOL	Manages 24/7 hotline, trains law enforcement agencies, participates in investigations	N/A	N/A
ITU	Sponsors IMPACT. Organizes conferences, releases guidelines and toolkits, facilitates information exchange and cooperation	Moderate	Internet usage and penetration statistics; secondary data from conferences and presented papers
NATO	Responding to military attacks on NATO member states	N/A	N/A: classified

(*Continued*)

Table 1. Continued.

Institution	Role	Data availability	Example variables (if applicable)
OECD	Develops policy options, organizes conferences, publishes guidelines and best practices	Low	Secondary data from conferences and presented papers
UNODC: United Nations Office on Drugs & Crime	Promotion of legislation, training programs, awareness, enforcement	N/A	N/A
WSIS	Global summit on information security; publishes resolutions and monitors implementation through stock-taking efforts	Low	Stock-taking database and secondary data from conferences and presented papers
US national entities			
NSA: National Security Agency	Shares Director, General Keith Alexander, with US CYBERCOM; specializes in cryptology services and research	N/A	N/A
CIA: Central Intelligence Agency	Defense of intelligence networks, information gathering	N/A	N/A: Classified
DHS	Protection of federal civil networks and critical infrastructure; information sharing and awareness; coordinating federal response and alerts	N/A	N/A: Unclassified data released through US-CERT
DoD: Department of Defense	Defense of military networks, counterattack capability	N/A	N/A: Classified
DOJ: US Department of Justice	Federal prosecution	Moderate	Non aggregated data: prosecuted cases, crime by industry
FBI	Federal investigation	Low	Total reported incidents, number of referrals to law enforcement agencies. Annual surveys on corporate computer crime including type and frequency of attacks, dollar loss, attack source
FTC	Consumer protection	N/A	N/A
IC3	Cybercrime reporting and referral center	High	Total complaints, referred complaints, estimated dollar loss, complaints by industrial sector
NW3C: National White Collar Crime Center	Provides training and support to law enforcement agencies, helps administer the IC3 with the FBI	N/A	N/A: statistics released through IC3

(*Continued*)

Table 1. Continued.

Institution	Role	Data availability	Example variables (if applicable)
FSSCC: Financial Services Sector Coordinating Council	By DHS mandate, identifies threats and promotes protection to protect financial sector critical infrastructure assets	N/A	N/A
Secret service	Investigation of economic cyber crimes	N/A	N/A
US-CERT	Defense of federal civil networks (.gov), information sharing and collaboration with private sector.	Moderate	Incidents and events by category, vulnerability reports
Non-US national entities (frequent collaborative partners)			
GCHQ: Government Communications Headquarters (UK)	One of three of Britain's intelligence agencies responsible for information assurance and cryptology; Britain's leading authority on cyber security	N/A	N/A
National Cyberdefence Centre (Germany)	Recently opened (16 June) agency for cyber security in Germany; responds to reports of cyber attacks on critical infrastructure	N/A	N/A
National Police Bureaus (e.g. Taiwan, South Korea, Japan, France)	Investigation, enforcement	Varies	Cases, arrests, prosecutions, demographics
Non-profits			
GICSR: Global Institute for Security and Research	Conducts R&D with industry leaders, public–private sector, and academia to develop policy and strategy for cyberspace	N/A	N/A
Internet society	Non-technical branch of Internet Engineering Task Force; provides leadership in addressing policy issues that confront the future of the Internet	N/A	N/A
CyberWatch	Develops educational programs and curriculum to train next generation of cyber security experts	N/A	N/A
CAIDA: Cooperative Association for Internet Data Analysis	Gathers data that will increase situational awareness of Internet topology structure, behavior, and vulnerabilities	High	Graphs and visuals of Internet traffic patterns
Private sector			
MacAfee	Industry leader in antivirus software; computer security services	Moderate	White papers

(*Continued*)

Table 1. Continued.

Institution	Role	Data availability	Example variables (if applicable)
PROINFO	Products analyze vulnerability dependencies and shows all possible attack paths into a network	N/A	N/A
Raytheon Co.	Cyber security solutions division offers wide arrange of information assurance services	N/A	N/A
Lockheed Martin	Defense contractor that supplies many governmental cyber security G&S	N/A	N/A
Red Tiger Security	Investigates cyber attacks	N/A	N/A
HB Gary	Investigates cyber attacks	N/A	N/A
Versigen iDefense	Investigates cyber attacks	N/A	N/A
International Computer Security Association	Specializes in antivirus, anti-spam, and firewall services among a wide array of other cyber security services	Moderate	Graphs of which countries sent the most spam per week

[a]N/A, not available.

appended to the organizations created to manage the aftermath of World War II and others were created specifically for meeting the development challenges.

3.1 *Sustainable development*

By 1990, the entire development discourse shifted away from *growth* per se (i.e. expansion of output) to *sustainable developmen*t (a more comprehensive and nuanced process). "Sustainability" had become central to our daily concerns as well as to policy and decision in all contexts and in nearly all parts of the world. Without undue simplification, it is fair to say that the traditional view of development focused on productivity and the expansion of economic output.

Later on concepts of human development took hold and the well-being of individuals and society were seen as essential features of development. Sustainable development, first formally introduced at the *United Nations Conference on Environment*, 1990, recognized the sanctity of nature and its life supporting services, thus placing the growth imperative in a broader context. *Agenda 21* framed and reflected an international consensus and a plan of action articulated in *Millennium Development Goals.* The view of sustainable development at the time was that of meeting the needs of present and future generations without undermining the cohesion of the social system or the life supporting properties of natural system.

During the last decade of the twentieth century, cyberspace was recognized almost universally as being of great importance. By an accident of chance, by design, or by the logic of technological development, this human-constructed environment had already assumed near worldwide scale and scope. Many parts of the world were still unconnected, but everyone recognized it was just a matter of time until the world's population became interlinked. It was an unstated assumption that the Internet would simply proliferate.

With the benefit of hindsight, we now appreciate that the assumption was correct, but also missed almost all of the underlying institutional dynamics, the emerging political contentions,

and the growing efforts of the state and the state system to shape trajectories, rules, and norms of a cyber system – with the Internet as its core – that had been built as an open domain, shaped by only the minimal regulatory conventions necessary for effective operation.

Unless proven otherwise, all evidence suggests that never before in modern times has a major technological innovation exhibited such rapid diffusion throughout the world. Differences in infrastructure, skills, literacy, and capabilities aside, cyber access in developing countries has expanded rapidly over the past decades.

During the early days of the Internet the open ethos dominated. With greater understanding of uses and growth in the diversity of users, networks were no longer secure. A wide range of malevolent intrusions with varying degrees of damage effects demonstrated without doubt the vulnerability of the Internet. With this near-certain vulnerability and threat, the very sustainability of the human-constructed cyber domain was at stake. Cyber security had now become a matter of national and, to the extent possible, international priority as well.

3.1.1 *Critical convergence of information and development*

The process shaping and managing the *World Summit on Information Society* (WSIS) places cyberspace at the center of international policy discourse. As a UN-based initiative, decisions at the WSIS were made at the state level, and only sovereign states served as "decision-makers." At the same time, all stakeholders wishing to participate in the overall process – from agenda setting to various forms and forums of deliberations – were encouraged to do so. This practice dated back to the United Nations Conference on Environment and Development in 1990, a major landmark in the history of international collaboration.

The WSIS intergovernmental initiative is a milestone in its own right as it sought to combine several distinct aspects of the UN's twentieth-century development agenda with emergent implications of information technology. WSIS was the first comprehensive response to the emergent "virtual" global society in a world increasingly concerned with the dilemmas of sustainable development. Although it was not conceived as a security-centric activity, the WSIS objectives that dealt with cyber security were broadly consistent with developmental concerns.

Operationally, WSIS was organized into two phases, each standing as a global conference in its own right. The first phase, held in Geneva in 2003, had representatives from over 175 countries committed to a wide-ranging action plan. Action Line C5 focused on "building confidence and security" and committed member countries to increasing security awareness, enacting legislation, and cooperating more extensively with the private sector (WSIS, 2003).

These goals were expanded upon in 2005 at the second phase in Tunis, when member organizations reaffirmed their Geneva commitments and agreed upon a collective stock-taking method to track action line implementation. The efforts by member states to implement Action Line C5 are viewable in a public database and are also published in annual reports (WSIS, 2009a). The combined conclusions transformed the general consensus into a Plan of Action. The Plan centered around information society in the developing world. This is the point of convergence between information and development.

At the WSIS meeting in Paris, 2013, we put forth the proposition that the overarching conditions for sustainability and for the process of sustainable development broadly defined rest not only on the sustainability of the social and the natural system, but also on the sustainability of the cyber system. In other words, sustainable development is contingent on the sustainability of all three systems – social, environmental, and cyber (Choucri, 2012). In other words, this proposition recognizes that humans are now embedded in three interconnected systems.

3.2 *The new security calculus*

Traditionally, national security focuses on security at the state borders and protection against military or other threatening intrusions. Over time this simple doctrine was refined into a more comprehensive view of security. In addition, the near universal expansion of government responsibility, the conception of a stable state, or alternatively, a failing one became closely tied to the evolving developmental agenda.

To simplify, security and sustainability gradually converged into one general vision of imperatives for survival, a vision that included border protection, social viability, and government capability. In its execution, defense was clearly the responsibility of the military. Social viability included, by emergent definitions, meeting the needs of present and future generations and the protection of nature's life supporting properties.

The construction of cyberspace created a new set of imperatives and an entirely new set of threats to security for the state system and all non-state entities – for profit and not for profit. No one could foresee the scale, scope, and damage potentials. Most important of all, the anonymity of the perpetrator created an unprecedented threat to both the traditional view of security, (defense of borders) and the revised view (military security, security of society and environment, and security of governance). Thus cyber security became a critical feature of overarching security, for industrial and developing states. It had to be managed at all levels of international relations – national, transnational, international, and global.

4. Computer Emergency Response Teams

New institutions were created specifically in response to cyber threats. These new institutions were created under national authority, with international scope, but not intergovernmental in form. Named *Computer Emergency Response Teams* (CERTs),[5] these are the only worldwide institutions created specifically in response to the new cyber threats. CERTs are an important addition to the dense network of international entities in the "real" or physical arena and occupy a salient role in the cyber security landscape.

As defined by the CERT Coordination Center (CERT/CC) – addressed later on – these entities focus on security emergencies, promote the use of valid security technology, and ensure network continuity (CERT Program, 2009a). In principle, this means that CERTs concentrate on identifying vulnerabilities and fostering communication between security vendors, users, and private organizations. Although the majority of CERTs were founded as non-profit organizations, many have transitioned toward public–private partnerships in recent years.

This type of lateral institutional design anchored in national governments attempts to build upon the successes of non-profit CERTs by providing a level of structure and resources hitherto unavailable. However, while the CERT network is becoming increasingly formalized, individual CERTs may differ considerably in their ability to effectively perform their mandates. By 2009, there were over 200 recognized CERTs, with widely different levels of organization, funding, and expertise (Forum of Incident Response and Security Teams [FIRST], 2009a).

At least three results are expected from CERT activities and interactions: a reduction in unaddressed security vulnerabilities, improved understanding of the nature and frequency of cyber threats, and enhanced communicating and reporting of incidents to other security teams and the general public. Although CERTs are not established to serve as information gathering institutions per se, their activities involve active threat monitoring and information exchange. As a result, many CERTs attempt to provide quantitative data for the cyber security community. To date, however, there is little effort to align or coordinate methods of data collection, and availability and reliability of reported information thus varies widely across the CERT

landscape. This means that the focus on organization has not yet extended to matters of performance and coordination.

4.1 *Organizational structure*

In general, CERTs share a common structure and backbone. In principle, this should help coordination. The majority of CERTs are organized according to guidelines originally published by CERT/CC, and many use common toolkits to establish their organizations (Killcrece, 2004). As a result, CERTs tend to differ from each other mainly in their area of focus (academic, private, national, and regional), or their respective area of expertise (phishing, viruses, and information security). These roles are largely self-defined based on each team's level of funding (which can vary widely), technical expertise, and the presence of perceived gaps within the CERT collaborative network. This means that the principle of autonomy supersedes that of collaboration.

The flexibility of this system greatly improves the possibility of coordination between CERTs; however, the loose network structure reduces the locus of responsibility or accountability for individual performance. In traditional institutional theory, the underlying generic objectives are to facilitate collective action, reduce transaction costs, and enable the performance of functions or the provision of services. To illustrate the complexity of arrangements, Figure 1 presents a subset of these structured relationships at different levels of analysis and organization.

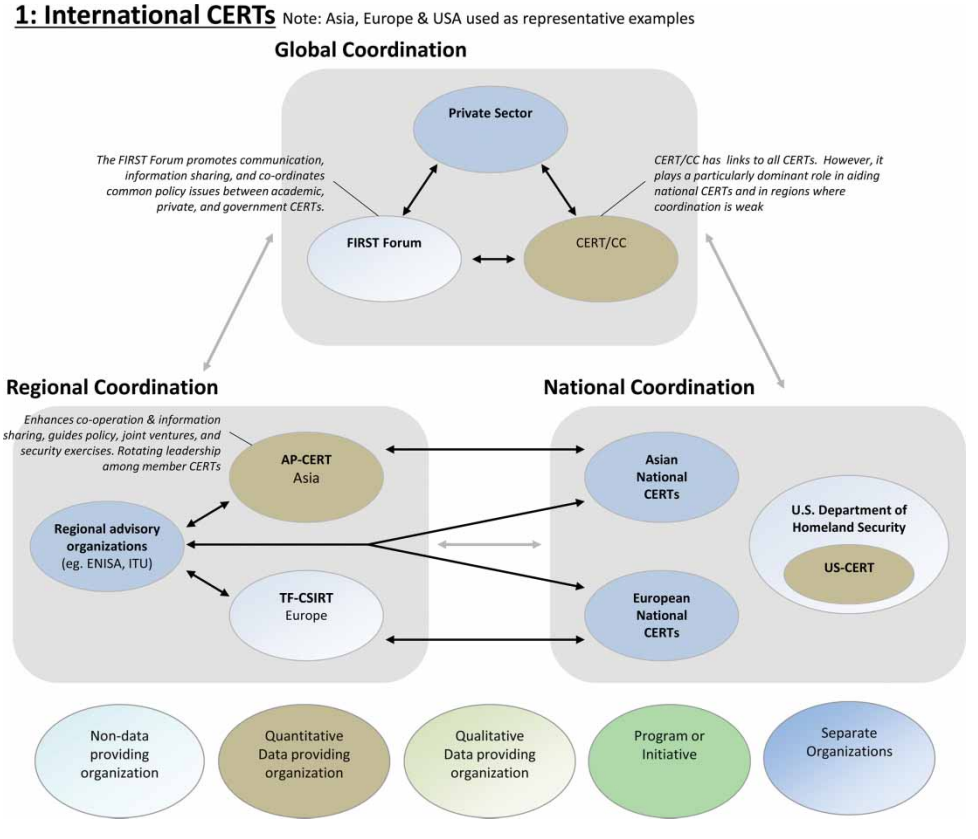

Figure 1. International CERTs.

4.2 *Coordinating organizations*

A distinguishing feature of the CERT system is its coordinating mechanism, CERT/CC, established at Carnegie Mellon University in 1998 – in response to a major Internet worm. CERT/CC was also the first operational CERT, and defined many functional parameters. The US Defense Advanced Research Projects Agency originally provided federal funding for the organization with the expectation that CERT/CC would serve as a center for direct threat assessment and response.

As cyberspace and cyber access expanded, a single organization proved insufficient to handle the increasing volume of security incidents. CERT/CC was forced to reframe its activities and priorities. Rather than responding directly to emerging incidents, CERT/CC's renewed mission utilized the lessons learned to provide guidelines, coordination, and standards for other CERTs. By relinquishing operational control in favor of a collaborative structure, CERT/CC laid the foundation for the establishment of regional, focused organizations. Today, the CERT network has expanded beyond the scope and control of CERT/CC, although CERT/CC continues to play an influential role in establishing national CERTs in developing countries and fostering inter-CERT communication.

In addition to CERT/CC, many CERTs also interact with parallel coordination networks, such as the *Forum of Incident Response and Security Teams* (FIRST). This body was established to enhance information sharing between disparate security groups (FIRST, 2009b). Now composed of more than 200 organizations, FIRST is notable for its influential annual conferences and its extensive integration of national, academic, and private CERTs (FIRST, 2009a). The establishment of these conferences in itself provides a basis for reinforcing communication and, as theory would suggest, enhances potentials for coordination.

4.3 *National CERTs*

The collaborative structure maintained by coordinating agencies such as FIRST and CERT/CC clearly facilitates information flow among security teams. But there were limitations. If CERTs were only organized in this fashion, it would be unclear which organizations possessed regional authority to coordinate the actions of other CERTs, for instance, in the event of a national attack on civilian networks. This problem was addressed by transitioning the CERT structure to the national level. One valuable side effect of this shift to national-level jurisdiction was the creation of public–private partnerships between national CERTs and existing national agencies.

But a solution to one problem can often give rise to additional complications. Given the diversity of national political systems and bureaucratic practices, the transition to national CERTs exacerbated the realities of legal and jurisdictional diversity. For example, while some national CERTs, such as US-CERT, were specifically tasked by their governments to defend civilian networks, other organizations operate in a legal vacuum and assume national responsibility via general consensus. Often, this legitimacy is granted by regional organizations such as Asia Pacific CERT (AP-CERT) in Asia and Task Force Computer Security Incident Response Teams (TF-CSIRTs) in Europe (Figure 1) that steer regional CERT policy. While this diversity is not necessarily a problem, it may impede information sharing, and it suggests that national CERTs may or may not be held to international operating standards.

Although national CERTs are endowed with regional authority, they remain restricted in their capacity to respond to cyber criminals. National CERTs occupy a first-line responder role in the event of attacks on national civilian networks, but lack the jurisdictional authority to shut down criminal networks and prosecute perpetrators. As a result, national CERTs focus primarily on responding to and preventing *technical* cyber threats – a necessary requisite for coordination but not a sufficient one.

In order to effectively deal with legal issues, clear lines of communication between national CERTs and government agencies are essential. This link has been formalized in some countries, such as the USA, but other nations are still developing the requisite connections between national CERTs and legal authority. At the same time, however, current CERT structure also includes vertical linkages – national, regional, and international connections – that are always difficult to forge but facilitate resilience and robustness of institutional performance over time.

4.4 *CERT data provision*

At this writing, the level of CERT cooperation and standardization does not extend to the collection or assessment of quantitative data. As suggested earlier, data availability varies widely among CERTs, and organizations that publish statistics do not necessarily use similar reporting methods (Madnick, Li, & Choucri, 2009). Moreover, there are no efforts underway to formally align and standardize metrics.

Overall, the lack of robust data can be traced to three underlying factors. First, it is inherently difficult to quantify cyber data due to uncertainties surrounding the nature, geographical location, and target of attacks. The rapid pace of technological development, coupled with a lack of standards-providing organizations has thus led to significant disparities in the diagnosis and classification of cyber events. Second, many CERTs lack a compelling business reason to gather or verify the accuracy of their quantitative data. CERTs typically possess limited funding capacity and many organizations choose to allocate their resources to cyber response in lieu of robust data collection. Lastly, there is no central authority or volunteer organization tasked with disseminating, collecting, or verifying CERT data. If there is an impediment to effective data use it is to be found in the domain of motivation – the foundations and the data are in place, but there appears to be little incentive in taking the next steps to disseminate gathered data. An initial step in this direction is reported in Madnick, Choucri, et al. (2009).

Although quantitative data are fragmented, the collaborative nature of the CERT network means that a significant amount of information remains available on CERT activities. From a research standpoint, CERT/CC and FIRST provide a means to analyze global CERT policy. In addition, CERT/CC provides a variety of data sources that can be used to evaluate historical CERT activity. These statistics include the number of security alerts, vulnerability notes, and advisories published per year. Although these figures are self-reported and the threshold necessary to publish an alert may vary from year to year, they provide a baseline for estimating global CERT activity. This analysis can be complemented by CERT/CC statistics on the number of incident reports and hotline calls received from member organizations and national CERTs.[6]

Useful data can also be gleaned by viewing aggregate data at the regional level. In particular, AP-CERT and several other regional bodies publish statistics that cover the number of incidents handled and reported, attack vectors, counts of defaced websites, and other Web vulnerabilities. While these statistics are not as robust as those provided by the private sector, they are partitioned along national lines and provide country-specific statistics that are valuable for analyzing divergent responses to cyber threats. By coupling this information with widely available metrics such as Internet connectivity or arrest rates, and controlling for data quality, it may be possible to develop a statistical model to analyze the overall effectiveness of cyber defense across nations, such as that illustrated in Madnick, Choucri, Li, and Ferwerda (2011).

CERTs occupy an important role in the international security ecosystem. But their core competencies or self-defined responsibilities do not extend to consensus building, legislation, or awareness-raising. This set of functions remained largely unclaimed in the early years of Internet development, but they have recently been embraced by a variety of intergovernmental organizations.

5. Intergovernmental responses

By definition, international organizations consist of sovereign states. All of the major international organizations and many minor ones were established long before the creation of cyberspace. They are all major users of cyber venues and often significant data providers as well. Unlike the CERTs, which are based on collaborative and hierarchical principles, intergovernmental organizations are composed of equal actors defined by their status as sovereign entities. All of these organizations are expected to be driven first and foremost by their own formal mandates and priorities. Thus, to the extent that any large international organization considers security in cyber venues as relevant to their concerns, it is mostly as a secondary priority. Given the pervasiveness of cyber venues, however, we expect that these organizations will devote increasing attention to cyber issues in the years to come.

If we focus on organizations that, in principle, have some clear interest or focus on cyberspace, we can identify the major actors and their zones of activity or interest. Unsurprisingly, this leads to a diffuse network of organizations and a wide array of cross-cutting linkages. By way of orientation, we show in Figure 2 several well-known international organizations (such as the UN) and new cyber-focused entities that do not have the status of "organization" but are likely to retain a long-standing institutional presence on the international arena (such as the WSIS).

5.1 *Early moves*

The involvement of international organizations in cyber security issues can be traced to early meetings of the G8 Subgroup on Hi-Tech Crime. In 1997, the G8, comprised of the world's

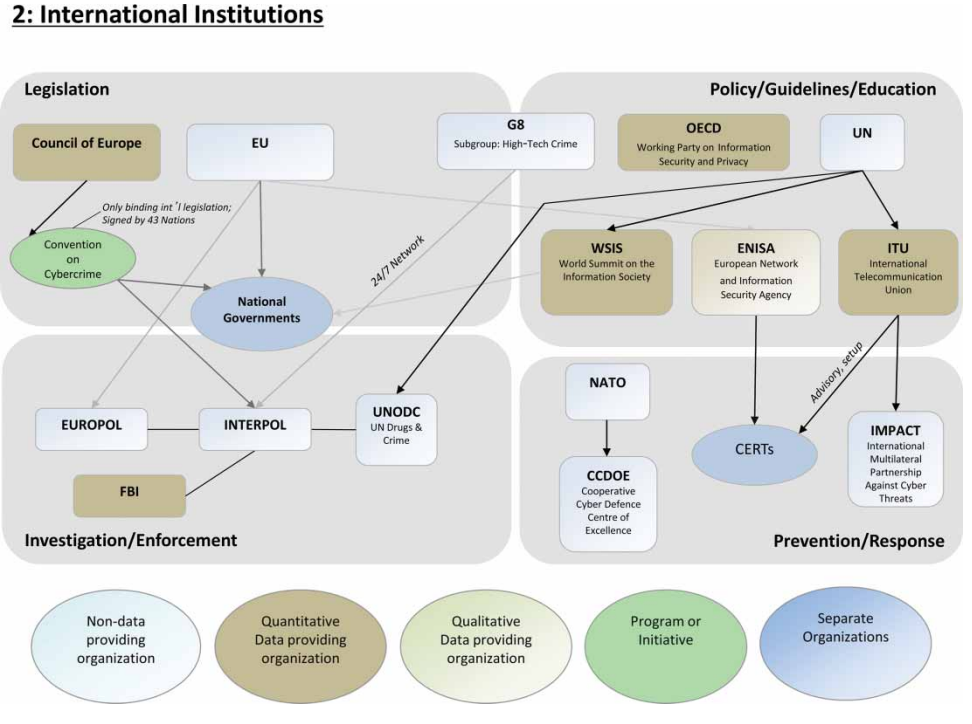

Figure 2. Key intergovernmental institutions.

most developed economies, established in cooperation with the International Criminal Police Organization (INTERPOL) a 24/7 "Network of Contacts" in order to help national governments "identify the source of terrorist communications, investigate threats and prevent future attacks" (G8 24/7 High Tech Contact Points, 2009). As part of the program, countries were asked to cooperate with INTERPOL in international investigations by sharing information on electronic crimes and by designating an official cybercrime point of contact. While the success rate of the program remains classified, a similar referral model was later mirrored by the Federal Bureau of Investigation (FBI) in the form of Internet Crime Complaint Center (IC3), which speaks to its relative success. As of 2007, 47 countries were actively involved within the network (Verdelho, 2008).

5.2 *Organisation for Economic Co-operation and Development-sponsored conferences*

The Organisation for Economic Co-operation and Development (OECD, 2009a) has been actively involved in the cyber security domain since 2002. Meeting twice a year in Paris, the *Working Party on Information Security and Privacy* (WPISP) has published several influential white papers, including "Guidelines for the Security of Information Systems and Networks" (2002) and "Promotion of a Culture of Security for Information Systems and Networks" (2005). These guidelines have been accompanied by stock-taking efforts that track the implementation of policy in member countries (OECD, 2009b). The WPISP has also released several surveys on information security policies in member countries and has created a "Culture of Security" Web portal for member states. Since the WPISP is contained within the OECD framework, it represents a formalized extension of OECD's core mission and provides a common approach for all member states.

For the most part, the foregoing efforts can be seen as "self-initiated," whereby private or public entities voluntarily take on a particular function in the emergent cyber security domain. However, more recently, the international community has issued operational mandates to specific organizations. Here, we note some of the most dominant initiatives.

5.3 *International Telecommunication Union*

One of *International Telecommunication Union's* (ITU, 2009b) core missions is to standardize telecommunication technology and release statistics that can be used to track the Internet connectivity of nations. Utilizing a group of high-level experts, ITU provides a variety of resources and toolkits addressing legislation, awareness, self-assessment, botnets, and CERTs (ITU, 2009a). Additionally, ITU publishes guides that educate developing nations on cybercrime and promote best practices and approaches.

Although the ITU core competencies are mission-specific, they have recently acted in a direct fashion by establishing an arm that will provide international threat response. The ITU was given the primary responsibility for coordinating the implementation of WSIS' Action Plan C5 (WSIS, 2009b). In response, the organization launched the "Global Cybersecurity Agenda" in 2007, working with the International Multilateral Partnership Against Cyber Threats (IMPACT), headquartered in Malaysia.

Envisioned as a global response center focused on combating cyber terrorism and protecting critical infrastructure networks, the *IMPACT* is a public–private venture headquartered in Malaysia (UNESCO, 2009). Among other services, IMPACT facilitates a real-time warning network to 191 member countries, 24/7 response centers, and the development of software that allows security organizations across the globe to pool resources and coordinate their defense efforts (IMPACT, 2009). Additionally, IMPACT maintains a research division, hosts

educational workshops, and conducts high-level security briefings with representatives of member states. These efforts are intended to make IMPACT the "the foremost cyber threat resource centre in the world" (ITU, 2009c).

Although IMPACT has only been operational since March 2009, it is likely that the organization will become a significant provider of technical security data in the near future. If this initiative is successful, an important precedent would be set for the proposition that an international organization can effectively perform a mission that lies beyond its initial cyber mandate, build upon its core competencies, and extend its regulatory domain in response to technological innovations. Its efforts to promote cyber security arose as a function of the increasing threat rather than as part of its original mission; thus, the international community chose to build upon existing organizational strengths rather than establishing a new institution.

5.4 *North Atlantic Treaty Organization*

A major adaptive initiative has been demonstrated by North Atlantic Treaty Organization (NATO) in a way roughly similar to IMPACT. Given the dramatic demonstration of cyber attacks against Estonia (an NATO member), this intergovernmental organization established a technical response arm in the aftermath of the coordinated attacks on Estonia in 2007. Designated the Cooperative Cyber Defence Centre of Excellence (CCDCOE, 2009), this entity is responsible for training NATO member states, conducting attack exercises, and supporting NATO in the event of an international cyber attack. Interestingly, not all NATO states have joined the CCDCOE program, with many countries opting to rely on their own traditional military cyber defense networks. There is no strong evidence that all members of NATO are willing to engage in a common approach to a shared problem, presumably because many states are developing their own strategies for cyber warfare. At the same time, however, the CCDCOE fills an important void for several European states, notably those whose own cyber security capabilities are yet to be developed.

5.5 *European Network and Information Security Agency*

All things considered, it is fair to conclude that the overall European technical response to cyber threats and cyber security has been somewhat limited in scope. Although the European Union has published numerous resolutions on cybercrime, and the European Police Office (EUROPOL) is actively engaged in investigation, the European Union's only substantive action thus far has been the creation of the European Network and Information Security Agency (ENISA). Tasked with a broad mandate "to enhance the capability of the European Union ... to prevent, address and respond to network and information security problems," ENISA largely focuses on awareness building, promoting Internet safety practices, and working with regional CERTs, and does not provide a comprehensive defense against regional cyber incidents (Europa, 2009).

5.6 *Convention on Cybercrime*

One area in which European organizations have taken the lead is within the legislative realm. In partnership with the USA, Japan, and others, the Council of Europe ratified the *Convention on Cybercrime* in 2004, which remains the only binding international legislation dealing with the cybercrime issue (Council of Europe, 2009a). As of September 2009, 26 countries have ratified the treaty, and an additional 20 countries have signed but not yet ratified (Council of Europe, 2009b). The Convention defines the criminality of cyber crime, enables law enforcement

agencies to effectively investigate electronic crimes, and fosters international cooperation and data sharing (Council of Europe, 2001).

In support of the Convention, the Council of Europe implemented two distinct action plans aimed at training law enforcement agencies and improving national legislation; it has hosted global conferences on cybercrime issues annually (Council of Europe, 2009c). Additionally, the Council of Europe maintains an extensive database on the progress of national cybercrime legislation (Council of Europe, 2009d). This growth in function is important as it provides evidence of institutionalized response and a broad framework necessary to effectively combat international cyber crime. However, it remains unclear whether the provisions of the Convention will be able to keep pace with the rapid development of the domain; international legislation is often reactive and generally lags behind technological efforts. The true value of the Convention may thus lie in its capacity to "jump-start" national cyber crime legislation via its provision of an adaptive legal framework.

5.7 *Data provision*

In this vein, many organizations provide valuable qualitative data, but few provide the quantitative statistics required for robust analysis. As a result, it is difficult to objectively determine the overall performance of these organizations.

This analytical gap may gradually close as organizations move from a passive posture to an active and fully engaged role within the security landscape, as is evident with the establishment of IMPACT and CCDCOE. Until then, the data provided by intergovernmental organizations can be most effectively used to trace the enactment of legislation, standards, and policies across member states. Utilizing stock-taking databases and ratification systems, it should be possible to determine which countries or regions are on the leading edge of enacting the necessary institutional frameworks to properly combat cyber crime.

Finally, it is important to stress that institutionalized data collection activities are always undertaken within a mission framework. In other words, collection of data is driven by the overall self-defined objectives and priorities of each organization. This is one of the major sources of non-comparability across data sets. So far, at least, we have not yet seen efforts to standardize definitions, collection procedures, or reporting mechanisms. In one sense, this is not an unexpected development, as information standardization usually takes place only after widespread data provision and demand.

6. National responses to security threats and cyber crime

Overall, theoretical approaches to institutions at the international level (generally addressed by scholars in the field of international relations) are based on historical and conceptual foundations different from those of institutional analysis at the national level (generally addressed by scholars in the field of comparative politics). While there are some common concerns and shared presumptions, the overall motivations, assumptions, and perspectives on the underlying problems differ considerably. Here, we do not need to explore the different epistemologies in any detail, suffice to note that in the most general terms, institutions in all contexts and at all levels of analysis are considered fundamental mechanisms of collective actions and that, at the very minimum, they reduce transaction costs, facilitate the provision of pubic goods, and enable the pursuit of social goals.

These core theoretical features are relevant to all institutional activities in response to cyber threats and cyber attacks; however, the theoretical foundations for understanding institutional

responses at the national level are based on domestic imperatives with little attention, if any, to international considerations (we shall return to this issue later on).

6.1 *Leading role*

The USA has been at the forefront of institutional response to the new realities formed by cyberspace. It is the leading world power, the state that originally encouraged and supported the creation of cyberspace, and the country that remains renowned for its innovative spirit. By default, the USA has been thrust in a leadership position and has acted as a model for other governmental response to cyber issues, notably in Europe and Asia. But, while the USA possesses arguably the strongest known national safeguards against various cyber threats, these programs appear to be far from sufficient. Indeed, according to a policy review, "it is doubtful that the United States can protect itself from the growing threat" by maintaining its current security structure (The White House, 2009a). The review continues:

> The Federal government is not organized to address this growing problem effectively now or in the future. Responsibilities for cybersecurity are distributed across a wide array of Federal departments and agencies, many with overlapping authorities, and none with sufficient decision authority to direct actions.

In order to trace the foundations of this institutional condition, we must turn to the early federal efforts to combat cyber vulnerabilities. The government initially delegated civilian network defense to the private sector or federally funded organizations such as CERT/CC. In parallel, the intelligence and military communities developed and maintained closeted defense systems. Although the relative technological advantage that these organizations possessed initially allowed them to maintain superiority over external threats, the lack of data sharing and cooperation among agencies, coupled with a rise in global technical competence, led to a growing security dilemma.

After the events of 2001, the USA began a substantial revision of its Internet security policy. Through a series of Presidential Directives, the nascent Department of Homeland Security (DHS) was granted responsibility for cyber Internet security efforts. These aims were codified in *The National Strategy to Secure Cyberspace* (2003), which led to a dual approach to cyber defense. With the cooperation of CERT/CC, a national CERT (US-CERT) was established within the National Cyber Security Division of the DHS and was tasked with defending federal civil networks (.gov domains). In order to coordinate the actions of various federal agencies, DHS was asked to develop contingency plans and warning systems, and was granted the ability to coordinate the efforts of 19 federal agencies in the event of a cyber attack of national significance (The White House, 2003). Notably, however, the document stressed that "the private sector is best equipped and structured to respond to an evolving cyber threat," and clearly delineated a separate approach for the "national security community" (The White House, 2003).

As a result, DHS assumed responsibility for a previously neglected area of defense (federal civil networks), but the compartmentalization of Internet defense strategies continued unchecked. However, it is important to note that this compartmentalization may be a normal byproduct of organizational and bureaucratic politics. As any legal scholar would be quick to point out, this segmentation is not an arbitrary development, rather it is supported by a legal framework delineating the discrete assignment of responsibilities.

The critical issue here is not that barriers to communication and information sharing – resulting from legal segmentation – create added constraints on rapid response to cyber threats. This situation is well appreciated by most, if not all, parts of the bureaucracy. Periodic restructuring initiatives have consolidated the security arena; however, these changes remain marginal given

the scale and scope of cyberspace and the associated threat potential. Nevertheless, the US government appeared committed to discovering valid alternatives, and there are several efforts underway that may result in an effective response structure.

6.2 *Emergent efforts*

US cyber policy was further refined in 2008, when President Bush signed a presidential directive establishing the CNCI, or the *Comprehensive National Cybersecurity Initiative*. The initiative includes several major policy revisions. First, in conjunction with the Office of Management and Budget, the DHS was tasked with reducing the number of network connections between federal agencies and external providers from 4000 to 50 within four months (Samson, 2008). Second, an optional DHS program that monitored traffic to and from federal websites, codenamed EINSTEIN, was transferred to the authority of the National Security Agency. The new version of the program purportedly captures content as well as traffic, and proactively monitors federal, and possibly private, networks (Samson, 2008). Lastly, the CNCI includes several provisions that are aimed at increasing R&D, coordinating cyber counterintelligence, and promoting information sharing among government organizations (The White House, 2009b).

Upon assuming office, President Obama endorsed the CNCI plan, albeit under conditions of increased transparency. Additionally, the White House authorized a sweeping review of cyber policy. Recognizing the increasing compartmentalization of national cyber defense, the final report recommended establishing a cyber security office within the White House. Leading this office, an official (referred to as the Cyber Czar by the press) would be a member of the National Security Council and would have frequent access to the President.[7] The office would not possess the authority to make policy unilaterally, but it would coordinate the responses of federal departments and attempt to bridge communication and policy gaps by

> "recommend[ing] coherent unified policy guidance where necessary in order to clarify authorities, roles, and responsibilities for cybersecurity-related activities across the Federal government" (The White House, 2009a).

Recognizing that "federal responses to cyber incidents have not been unified," the review recommended eliminating overlapping responsibilities between agencies and defining specific roles for cyber defense across government networks (The White House, 2009b).

These recommendations are still in the process of being implemented. However, considerable strides have been made in providing a coherent logic and rationale for the overall organizational response system. The proposed structure is presented in Figure 3.

The transition from an organic, overlapping defense network to organized hierarchies can best be observed as a recurring pattern within the cyber security landscape. However, while centralization and coordination is necessary in order to effectively respond to rapidly evolving threats, inefficient organizational structures may confound the problem by reinforcing barriers to bureaucratic adaptation. While few governments are as large and complex as that of the USA, the fact remains that US cyber policies and the mechanisms for their implementation provide important signals to other governments. Even if the US response does not serve as a formal model, its institutional responses will be closely scrutinized by others.

6.3 *Cyber crime*

The USA is a signatory to the Convention on Cyber Crime, with reservations. An important case of organizational restructuring in response to cyber threats is illustrated by its own responses to

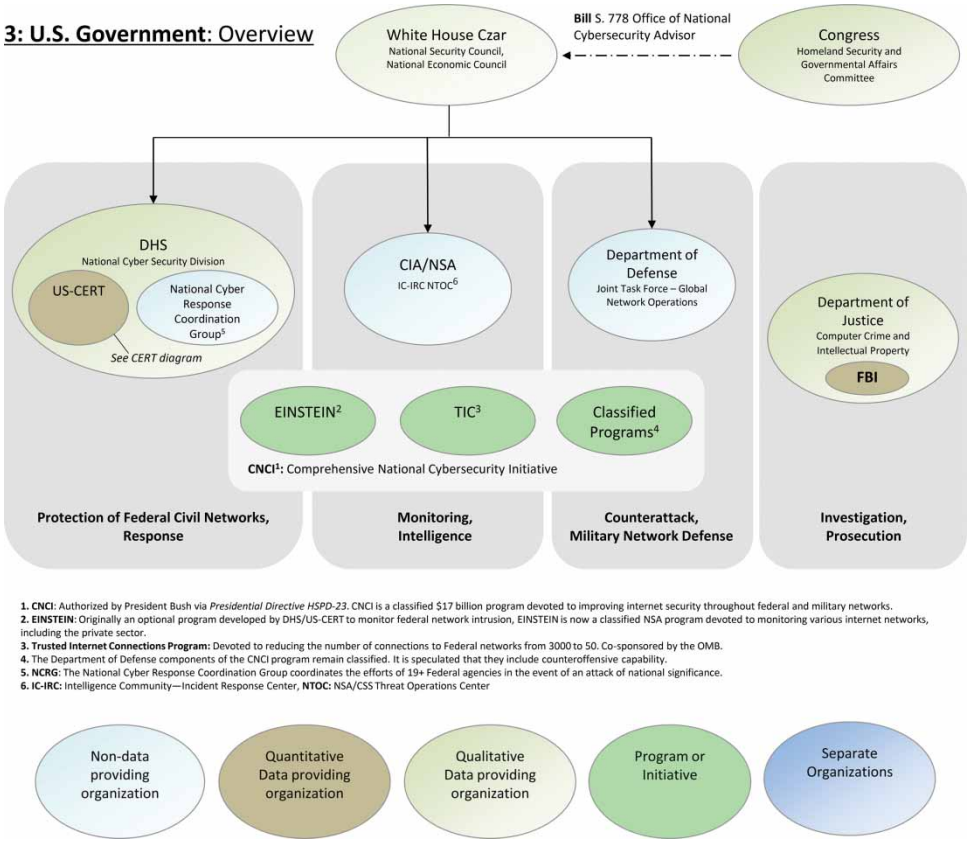

Figure 3. Proposed US structure.

the threats of 2001, when the FBI collaborated with the National White Collar Crime Center to form the IC3. Sharing some structural similarities with INTERPOL's 24/7 network, IC3 was created to provide a central contact point for reporting Internet crimes. The program is still active today, and by most accounts, has been a success. In 2008 alone, the IC3 processed over 275,000 complaints, 26% of which were deemed valid and referred to law enforcement agencies (National White Collar Crime Center, 2008). However, while the organization serves as a successful model for a national reporting system, this model has been unable to constrain the growth of cyber crime. FBI surveys have shown that most Internet crime remains unreported, and only a fraction of total cyber incidents are processed by the IC3. Furthermore, although the estimated dollar loss of cybercrime has increased every year since 2005, referrals have decreased substantially during the same period (National White Collar Crime Center, 2008).

In some sense, the lack of dramatic success thus far is unsurprising. Efforts to halt the spread of cyber crime suffer from a number of inherent challenges. First, in contrast with traditional crime, the criminality of cyber activities remains ill-defined. Many individuals are not accustomed to reporting cyber crime to law enforcement organizations because issues may be deemed "minor" or purely technical in nature, or because events on the Internet are deemed outside the jurisdiction of a local police agency. This issue is present in the corporate sphere as well, as many companies view the public acknowledgement of security vulnerabilities as a

corporate liability. Second, even when crimes are reported, investigation and prosecution remains difficult. Evidence is often ephemeral and transitory, and the global nature of cyber crime presents serious difficulties in pinpointing the location and identity of criminals. Lastly, it often proves difficult to assess the true monetary damage of cyber crime, for instance, in the case of information theft or security breach. Given that law enforcement agencies possess limited resources, this ambiguity surrounding the true impact of cyber crime creates difficulties in setting investigative priorities.

Although many of the efforts of the FBI and the Department of Justice (DOJ) have focused on combating cyber crime at the national level, some initiatives have attempted to ameliorate some of the aforementioned problems by embedding cyber crime experts in local institutions. For instance, since 2003 the FBI has established collaborative Computer Crime Task Forces, which assist police agencies in investigating local cyber crimes. As of 2006, there are over 92 task forces spread throughout the USA (Federal Bureau of Investigation, 2006). In a similar vein, the DOJ has established Computer Hacking & Intellectual Property units in local federal courts, which provide lawyers with the training to effectively understand and prosecute cyber crime.

In recent years, the Federal Trade Commission (FTC) has also played an active role in preventing the spread of cyber crime. This new area of focus was not specifically mandated, but rather arose as a byproduct of efforts to expand the FTC's role in consumer protection. Although the FTC is not tasked with prosecuting or investigating criminal networks, the commission acts by issuing formal complaints and restraining orders against Internet Service Providers (ISPs) that are suspected of hosting or promoting illegal activity. These actions prevent ongoing cyber crime activities, while prosecution efforts are underway. The FTC thus occupies a critical role in cross-sector collaboration, as the organization possesses the legal authority to rapidly respond to time-sensitive security alerts from NGOs, CERTs, and local government agencies.[8]

In many ways, the USA is simultaneously pursuing centralized and decentralized approaches to combating cyber crime (Figure 3). Critical to the success of either approach is the establishment of a national culture that understands, recognizes, and reports cyber crime. Although statistics on the success of local efforts remain limited, it is important to recognize that initial investments in the sector may not display immediate dividends, due to the necessities of preliminary education and training (Figure 4).

The ITU comparison of cyber security initiatives worldwide revealed a wide range of approaches with different degrees of development (ITU, 2005). While the process of institutionalizing responses to cyber threats is at an early stage, it is possible to discern possible emergent trajectories via the use of (highly incomplete) quantitative data provided by national governments. It is unlikely that governments will publically release data related to national security intrusions, and data relating to civilian criminal activities is only available for a select few countries.

For example, in the USA, the DOJ maintains a partial database of high-profile cases and convictions, while the FBI regularly publishes IC3 and survey data on cyber crime trends.[9] Similarly, national governments in Korea, Japan, and Taiwan release comprehensive yearly statistics on cyber crime investigations, prosecutions, arrests, and demographic data. Although less directly available, statistics are also provided by countries such as the UK, Germany, and France.

Unfortunately, however, many countries lack robust legislation dealing with cyber crime; as a result, cyber crime is rarely reported as a distinct category within national police reports. Until such time that additional countries ratify the Convention on Cybercrime – and governments actively pursue its implementation – it is probable that cybercrime data will not become more widely available.

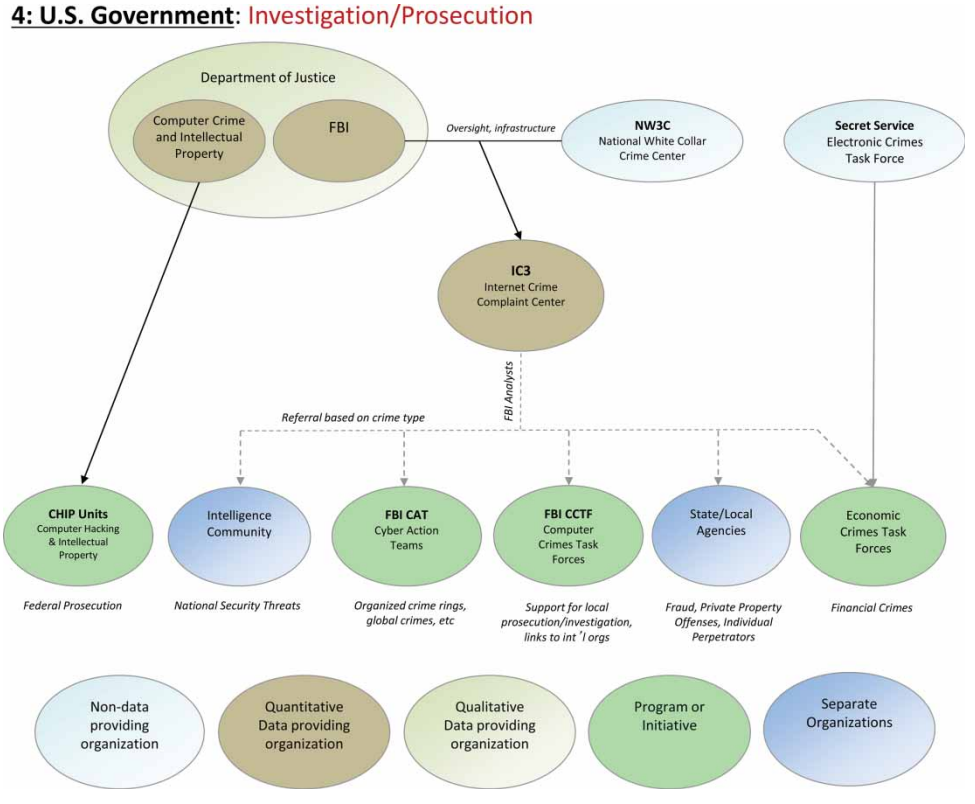

Figure 4. US investigation/prosecution organizations.

7. Some baseline conclusions

As presented above, the institutional cyber security landscape consists of a complex array of organizations that exhibit significant diversity with regard to missions, mandates, interests, opportunities, and constraints.

7.1 *Characteristic features*

On these bases, we put forth the following observations:

(a) The information technology-sustainable development linkage has become an integral feature of the international community's policy priorities.
(b) The current institutional landscape resembles a security patchwork that covers critical areas rather than an umbrella that spans all of the known modes and sources of cyber threat.
(c) Given the multiple contexts and diverse institutional motivations, we expect that responses will be driven more by institutional imperatives and reactions to crisis than by coordinated assessment and proactive response.
(d) Due to the complex global agenda at all levels of development, states may not be willing to proceed until international norms are developed, rather they will "take matters in their own hands" and develop first-order responses.

(e) Cross-sector collaboration among public, private, and volunteer organizations may serve as a temporary measure to cover holes in the current defense network. However, at some point effective institutions will be necessary; they may develop in parallel with rising public awareness.
(f) So far, we have not yet seen large terrorist groups engaged in intense cyber malfeasance. This pattern cannot be expected to continue. Efforts to infiltrate critical US infrastructure and the devastating attacks on Estonia and Georgia in 2007 and 2008 underline the dangers of being lulled into a false sense of security. As the Internet becomes increasingly central to modern society, it is likely that criminals, terrorist groups, and other opponents to state authority will target this sector in the hopes of disrupting critical national functions. So far, the potential for significant threats is far greater than institutional capabilities to contain these threats. In other words, the "demand" for security far exceeds the provision of effective "supply."

7.2 *Institutional anchors for cyber security*

Such features notwithstanding, based on the evidence to date, we suggest that considerable strides have been made to establish foundations for collaborative responses. In the best of all possible worlds, we would expect to see the emergence of a collaborative framework – a large umbrella network – allowing autonomous organizations to flexibly adapt to emerging threats in a coordinated manner and increasing the impetus for information sharing in the realm of cyber security. While the potential for such an umbrella network has yet to be realized, we can now point to some institutional anchors that could support, or even consolidate, such a development:

(a) The establishment of not-for-profit institutions designed to focus on cyber threats (CERT/CC, FIRST, and private CERTs), however "disorganized," is a growing trend on the international landscape. In some instances, these institutions have transitioned to private–public partnerships.
(b) A number of international institutions established to manage interactions among advanced states (notably supported by the OECD) reinforce rather than undermine this development.
(c) International conferences designed to communicate the potential for information technology to facilitate transitions toward sustainable development (WSIS), while not centered on security issues, nonetheless have the advantage of large-scale private and public participation, thus raising the political profile of cyber issues globally.
(d) The functional international organizations with core missions and competencies (notably the ITU) have adopted security as part of their missions.
(e) Despite these seemingly complex and uncoordinated responses at the national level, specific agencies are more and more tasked with responding to cyber crime (notably the FBI in the USA).
(f) The development of binding international legislation (i.e. the Convention on Cybercrime) elevates the sense of vulnerability as well as the need to coordinate responses to a higher level of awareness than ever before.
(g) In the field of military security framed more formally, we observe the salience of organizations and strategies focused on the defense of military and intelligence networks (i.e. CCDOE, CNCI).

Each of these institutional responses reflects mandates, rules, and responsibilities. None are accorded complete regulatory power. Indeed, there is little evidence of overarching institutional coordination or routinization. On the one hand, this pattern represents a certain degree of

disconnect. On the other, it can be seen as a dynamic and shifting response to dynamic set of cyber threats. In the latter context, one could argue that the increasingly dense landscape of institutional responses is an excellent indication that the international community is taking serious steps to control a cyber threat of epidemic proportions.

In this connection, we can expect that, over time, we will see more and more forms of lateral intergovernmental cooperation with the requisite institutional cross-border institutional collaboration. The theoretical foundations for such developments are accommodated by the structure of the process of transnational activities as framed by Nye and Keohane (1977) and the extensions in transnational governance outlined by Slaughter (2004) in the context of globalization processes.

7.3 *Critical missing piece*

Although the current system of institutional arrangements shows signs of weakness, it is also true that the level of organization and cooperation has been steadily increasing. Missing from these international institutional developments (and thus from the above analysis) is a critical piece of institutional architecture to support a fundamental function, namely systematic consideration for data issues and matters of data provision and alignment. To some degree, the effectiveness of this effort can be quantified through the use of statistics.

While a relatively small number of organizations produce reliable data, sufficient information exists to develop a model that maps degree of vulnerability versus the effectiveness of organizational response. For instance, international data on cyber crime legislation and awareness can be correlated with arrest rates in individual countries. When combined with stock-taking databases, this method allows one to determine the rate of progress in individual nations versus cybercrime issues. Similarly, quantitative data provided by national CERTs can be used to obtain insights about their performance in their respective national contexts and constituencies. An example of these kinds of analysis, along with a Data Dashboard tool, can be found in the report (Madnick, Li, et al., 2009).

Over time, we anticipate the possibility of pairing international and national statistics with information from the private sector. Security and monitoring companies such as Symantec, Arbor Networks, Microsoft, and McAfee provide quantitative data that address the global spread of Internet vulnerabilities. In many cases, the volume and quality of data released by these organizations far outpaces the information released by international and national organizations; however, the true value of this information lies not in an isolated analysis, but in the intersection of private data with the national and international sphere. For instance, statistics concerning the originating country of cyber attacks or the absolute volume of attacks can potentially be paired with national CERT data to determine the degree of national vulnerabilities and traffic that each CERT is capable of handling.

These metrics, and others that can potentially be derived, may provide a powerful method of simultaneously evaluating data quality and organizational performance. An important next step in our inquiry is to examine additional data providers and explore ways of pairing this data with national and international organizations to form evaluative statistical models. While doing so, it is important to remain cognizant of the institutional context that enables or constrains the provision of information.

Acknowledgements

Any opinions, findings, and conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the Office of Naval Research.

Funding

The work reported herein was supported, in part, by the Explorations in Cyber International Relations (ECIR), the Office of Naval Research (ONR) [contract number N00014-09-1-0597].

Notes

1. See, for example, Goodrich, (1947), Claude (1967), and Hoffmann (1987).
2. See, for example, Mitrany (1948).
3. Haas (1961) is a good example.
4. See Keohane (1983) as an example. The concept of regime emerged as an important anchor in the field.
5. These organizations are also referred to as Computer Security Incident Response Teams (CSIRTs).
6. Unfortunately, CERT/CC has announced that no statistics will be published after Q3 2008. As a result, analysis is limited to historical applications (1988–2008).
7. Note that the position has been established and is currently filled by Michael Daniel.
8. These are all examples of institutional developments in response to cyber security threats.
9. Note, however, that the USA does not currently provide any comprehensive statistics on arrests or prosecutions.

Notes on Contributors

Nazli Choucri is a Professor of Political Science at the Massachusetts Institute of Technology. Her research concentrates on sources and consequences of international transformations and change, with a focus on types of international conflict and modes of cooperation. She is the Principal Investigator of a multi-year, multi-disciplinary research project of MIT and Harvard University on Explorations in Cyber International Relations and Director of the Global System for Sustainable Development (GSSD), a multi-lingual web-based knowledge networking system focusing on the multi-dimensionality of sustainability. She is the founding Editor of the MIT Press Series on Global Environmental Accord and the former General Editor of the *International Political Science Review*. Her most recent book, *Cyberpolitics in International Relations*, was published by the MIT Press in 2012.

Dr. Stuart Madnick is the John Norris Maguire Professor of Information Technology at the Sloan School of Management and Professor of Engineering Systems in the School of Engineering at the Massachusetts Institute of Technology (MIT). He has degrees in Electrical Engineering (B.S. and M.S.), Management (M.S.), and Computer Science (Ph.D.) all from MIT. His current research interests include connectivity among disparate distributed information systems, database technology, software project management, cybersecurity, and the strategic use of information technology. He is the author or co-author of over 380 books, chapters, articles, or technical reports on these and related topics. He has also been active in industry as a consultant and co-founder of several companies.

Jeremy Ferwerda is a PhD Candidate in the Department of Political Science at the Massachusetts Institute of Technology. Prior to attending MIT, he graduated summa cum laude from Cornell University with degrees in History and Biological Sciences, and worked as a financial analyst for a hedge fund.

References

CERT Program. (2009a). *About CERT*. Retrieved September 17, 2009, from http://www.cert.org/meet_cert/

Charney, S. (2009). *Rethinking the cyber threat: A framework and path forward*. Retrieved from http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=747

Choucri, N. (2012). *Cyberpolitics in international relations*. Cambridge, MA: MIT Press.

Claude, I. L., Jr. (1967). Collective legitimization as a political function of the United Nations. In O. R. Young (Ed.), *The international political economy and international institutions, volume 1* (pp. 22–52). Cheltenham: Edward Elgar Publishing Limited.

Cooperative Cyber Defence Centre of Excellence. (2013). Retrieved January 11, 2009, from http://www.ccdcoe.org/

Council of Europe. (2001). *ETS No. 185 – convention on cybercrime*. Retrieved September 19, 2009, from http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Council of Europe. (2009a). *Council of Europe action against economic crime*. Retrieved September 28, 2009, from http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Default_en.asp
Council of Europe. (2009b). *Convention on cybercrime*. Retrieved September 27, 2009, from http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=09/09/2009&CL=ENG
Council of Europe. (2009c). *Project on cybercrime (phase 1)*. Retrieved September 26, 2009, from http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime%5Ccy%20Project/projectcyber_en.asp
Council of Europe. (2009d). *Cybercrime legislation – country profiles*. Retrieved September 28, 2009, from http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp
Europa. (2009). *European Network and Information Security Agency (ENISA)*. Retrieved September 21, 2009, from http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l24153_en.htm
Federal Bureau of Investigation. (2006). *Netting cyber criminals*. Retrieved February 20, 2010, from http://www.fbi.gov/page2/jan06/ccctf012506.htm
Forum of Incident Response and Security Teams. (2009a). *Alphabetical list of FIRST members*. Retrieved September 20, 2009, from http://www.first.org/members/teams/
Forum of Incident Response and Security Teams. (2009b). *FIRST history*. Retrieved September 29, 2009, from http://www.first.org/about/history/
Goodrich, L. M. (1947). From League of Nations to United Nations. In O. R. Young (Ed.), *The international political economy and international institutions, volume 1* (pp. 22–52). Cheltenham: Edward Elgar Publishing Limited.
G8 24/7 High Tech Contact Points. *Cyber security co-operation*. Retrieved October 28, 2009, from http://www.cybersecuritycooperation.org/moredocuments/24%20Hour%20Network/24%207%20invitation.pdf
Haas, E. B. (1961). International integration: The European and the universal process. In O. R. Young (Ed.), *The international political economy and international institutions, volume 1* (pp. 22–52). Cheltenham: Edward Elgar Publishing Limited.
Hall, P. A., & Taylor, R. C. R. (1996). Political science and the three new institutionalisms. *Political Studies*, *44*(5), 936–957.
Hansen, D. L., Bertot, J. C., & Jaeger, P. T. (2011). Government policies of the use of social media: Legislating for change. In John Bertot & Karine Nahon (Eds.), *Proceedings of the 12th annual international conference on digital government* (pp. 131–140). College Park, MD.
Hoffmann, S. (1987). International organization and the international system. In O. R. Young (Ed.), *The international political economy and international institutions, volume 1* (pp. 22–52). Cheltenham: Edward Elgar Publishing Limited.
IMPACT. (2009). *Welcome to the coalition*. Retrieved October 23, 2009, from http://www.impact-alliance.org/
International Telecommunication Union. (2005). *A comparative analysis of cybersecurity initiatives worldwide*. Retrieved December 16, 2011, from http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf
International Telecommunication Union. (2009a). *Global Cybersecurity Agenda (GCA)*. Retrieved September 25, 2009, from http://www.itu.int/osg/csd/cybersecurity/gca/
International Telecommunication Union. (2009b). *Information and communication technology (ICT) statistics*. Retrieved September 25, 2009, from http://www.itu.int/ITU-D/ict/
International Telecommunication Union. (2009c). *Global Cybersecurity Agenda (GCA): Technical and security measures*. Retrieved September 25, 2009, from http://www.itu.int/osg/csd/cybersecurity/gca/tech-proced.html
Keohane, R. O. (1983). The demand for international regimes. In O. R. Young (Ed.), *The international political economy and international institutions, volume 1* (pp. 22–52). Cheltenham: Edward Elgar.
Killcrece, G. (2004). *Steps for creating national CERTs*. Carnegie Mellon Software Engineering Institute. Retrieved September 13, 2009, from http://www.cert.org/archive/pdf/NationalCSIRTs.pdf
Lowi, T. J. (1964). American business, public policy, case studies, and political theory. *World Politics*, *16*(4), 677–715.
Madnick, S., Choucri, N., Camina, S., Fogg, E., Li, X., & Wei, F. (2009, August). *Explorations in Cyber International Relations (ECIR) – Data Dashboard Report #1: CERT Data Sources and Prototype Dashboard System*. Cambridge, MA: Sloan School of Management, MIT (Sloan School of Management Working Paper SWP #4754–09).
Madnick, S., Choucri, N., Li, X., & Ferwerda, J. (2011, December 3–4). Comparative analysis of cybersecurity metrics to develop new hypotheses. In Karin Hedström, Fredrik Karlsson, & Zhengchuan

Xu (Eds.), *Proceedings of the workshop on information security & privacy, (Jointly hosted by AIS SIGSEC and IFIP TC11.1)*. Shanghai: Association of Information Systems Special Interest Group on Information Security and Privacy.

Madnick, S., Li, X., & Choucri, N. (2009, December). Experiences and challenges with using CERT data to analyze international cyber security. In Merrill Warkentin & Rita Walczuch (Eds.), *Proceedings of the AIS SIGSEC Workshop on Information Security & Privacy* (pp. 6–16). Phoenix, AZ: Association of Information Systems Special Interest Group on Information Security and Privacy.

Mitrany, D. (1948). The functional approach to world organization. In O. R. Young (Ed.), *The international political economy and international institutions, volume 1* (pp. 22–52). Cheltenham: Edward Elgar Publishing Limited.

National White Collar Crime Center. (2008). *IC3 annual report*. Retrieved September 23, 2009, from http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf

Nye, J. S., & Keohane, R. O. (1977). *Power and interdependence: World politics in transition*. Boston, MA: Little, Brown and Company.

OECD. (2009a). *What is the Working Party on Information Security and Privacy (WPISP)?* Retrieved October 23, 2009, from http://www.oecd.org/document/46/0,3343,en_2649_34255_36862382_1_1_1_1,00.html

OECD. (2009b). *Initiatives by country*. Retrieved September 27, 2009, from http://www.oecd.org/document/63/0,3343,en_21571361_36139259_36306559_1_1_1_1,00.html

Reich, S. (2000). The four faces of institutionalism: Public policy and a pluralistic perspective. *Governance*, *13*(4), 501–522.

Samson, V. (2008, July 23). *The murky waters of the White House's cybersecurity plan*. Center for Defense Information. Retrieved September 26, 2009, from http://www.cdi.org/program/document.cfm?DocumentID=4345&from_page=../index.cfm

Slaughter, A.-M. (2004). Disaggregated sovereignty: Towards the public accountability of global government networks. *Government and Opposition*, *39*(2), 159–190.

The White House. (2003). *The National Strategy to Secure Cyberspace*. Retrieved September 20, 2009, from http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

The White House. (2009a). *Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure*. Retrieved September 23, 2009, from http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

The White House. (2009b). *The comprehensive national cybersecurity initiative*. Retrieved March 20, 2010, from http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

UNESCO. (2009, March 23). *UN-backed anti-cyber-threat coalition launches headquarters in Malaysia*. Retrieved March 24, 2009, from http://portal.unesco.org/ci/en/ev.php-URL_ID=28464&URL_DO=DO_TOPIC&URL_SECTION=201.html

Verdelho, P. (2008). *The effectiveness of international co-operation against cybercrime*. Council of Europe. Retrieved September 27, 2009, from http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/DOC-567study4-Version7_en.PDF/

WPISP. (2002). *OECD guidelines for the security of information systems and networks: Towards a culture of security*. Paris: OECD.

WPISP. (2005). *The promotion of a culture of security for information systems and networks in OECD countries*. Paris: OECD.

WSIS. (2003). *Plan of action.* Retrieved October 17, 2009, from http://www.itu.int/wsis/docs/geneva/official/poa.html

WSIS. (2009a). *Stocktaking*. Retrieved October 17, 2009, from http://www.itu.int/wsis/stocktaking/index.html

WSIS. (2009b). *WSIS C5*. Retrieved October 17, 2009, from http://www.itu.int/osg/csd/cybersecurity/WSIS/