

Cyber Security: ³⁸¹¹⁷

A New Model for Protecting the Network



In a networked world, there are no real safe harbors—if you are on the network, you are available to everyone else on the network.¹ As economies become more dependent on information and communications technology (ICT), they are becoming more vulnerable to network attacks (e.g., threats to the Internet, as well as other private and public networks). The most serious cyber security risks are those that threaten the functioning of critical information infrastructures,² such as those dedicated to financial services,³ control systems for power, gas, drinking water, and other utilities; airport and air traffic control systems; logistics systems; and government services.⁴

Although the prevailing rationale for cyber security is to ensure a favorable climate for ICT investment, national and international security concerns are becoming equally important rationales. In the developing world, foreign direct investment as a whole may eventually be affected by the safety and integrity of data networks available to investors in host countries. In advanced industrial nations, basic public trust in modern economies and the electronic networks on which they depend is eroded when electronic data is stolen, becomes corrupted, or can no longer be authenticated.

¹ This paper and the larger study on which it is based, “International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues” (Delft, The Netherlands: TNO Information and Communication Technology, 2005, available online at <http://cds-1.dartmouth.edu/tiki> [accessed July 2006]) were made possible by a learning and sharing grant from the Dutch Trust Fund of the Global Information and Communication Technologies Department and from funds from the Legal Department of the World Bank through LEGPS. The authors included Robert Bruce (Center for Digital Strategies, Tuck School of Business at Dartmouth), Scott Dynes (Center for Digital Strategies Tuck School of Business at Dartmouth), Hans Brechbuhl (Center for Digital Strategies, Tuck School of Business at Dartmouth), Bill Brown (Institute for Security Technology Studies, Dartmouth College), Eric Goetz (Institute for Information Infrastructure Protection, Dartmouth College), Pascal Verhoest (TNO Information and Communication Technology), Eric Luijff (TNO Defense, Security and Safety), and Sandra Helmus (TNO Information and Communication Technology). Robert Schware of the World Bank’s Global ICT Department managed the project (rschware@worldbank.org).

² See the definition of critical infrastructures in European Union, “Critical Infrastructure Protection in the Fight against Terrorism,” COM(2004) 702 Final, Communication from the Commission to the Council and the European Parliament, European Union, Brussels, 2004.

³ For information on how the financial services sector looks at cyber threats, see the website of BITS, a financial service industry consortium, <http://www.bitsinfo.org> (accessed July 2006).

⁴ The U.S. National Infrastructure Advisory Council (NIAC) identifies eight such critical infrastructures: power, water, transportation, communications, financial, manufacturing, emergency services (fire, police, 911), and health care. For background information on NIAC, see the website of the U.S. Department of Homeland Security, http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0353.xml (accessed July 2006).

Cyber security is thus a collective concern that is comprehensive in scope—the Internet has no national boundaries. Whereas security is typically regulated at the government level, cyber security is at once national, international, public and private in character. In fact, the capacity for cyber risk management and security lies largely in the hands of private entities that manage and operate most ICT infrastructure. Such security cannot be adequately assured by market forces or regulation; rather, it requires a novel mix of solutions involving a range of stakeholders working both in their own domains and in concert.

No single strategy, set of governance arrangements, or operational practices will be right for every country. However, it is imperative that countries develop improved lines of communication based on trust to discuss cyber security both within and among themselves.

CYBER-SECURITY RISKS

New risk factors and challenges to data and communications networks seem to be evolving as rapidly as the spread of high-speed Internet infrastructure. Among these compelling risks are:

Computer worms and viruses. Debilitating worms and computer viruses have demonstrated destructive capabilities for a number of years, as evidenced by the damage caused by such programs as Sasser, Blaster, Netsky, Welchia and Code Red.⁵

Organized criminal activity. The booming growth of ICT-services has spawned new gray-and black-market opportunities that organized criminal elements are exploiting for huge financial advantage. Financial institutions, for example, have already experienced significant losses through “phishing” and “pharming” operations.⁶ The more significant the volume of revenues that flow over ICT-based networks, the greater will be the incentive for organized criminal elements to corrupt or economically exploit high-value data resources.⁷ A global “black economy” can, for example, generate financing for terrorism,⁸ as well as “off-budget” funding for military, police, or national security agencies of nation states.

⁵ In China, for example, CCERT, the organization created in 1999 to monitor spam and provide security-related and emergency response services, recorded 28,424 incident reports in 2003. The volume of incidents in 2003 was more than twice that recorded in 2002 and consisted primarily of computer viruses and worms (62.87%) and spam (18.49%). See CNCERT/CC Annual Report 2004 on website of the Ministry of Information Industry of China, http://www.cert.org.cn/english_web/document/2004CNCERTCCAnnualReport.pdf (accessed July 2006).

⁶ *Phishing* is the act of sending an e-mail that claims to be from an established legitimate enterprise in an attempt to scam a user into surrendering private information for the purposes of identity theft. *Pharming* seeks to obtain personal or private (usually financial-related) information by creating false websites (domain spoofing). For information on trends and counter-measures to combat phishing and pharming, visit the website of the Anti-Phishing Working Group, an industry association in California, <http://www.antiphishing.org> (accessed July 2006).

⁷ See, for example, Brian Krebs, “Phishing Feeds Internet Black Markets,” *The Washington Post*, November 14, 2004, <http://www.washingtonpost.com/wp-dyn/articles/A59347-2004Nov18.html> (accessed July 2006).

⁸ Imam Samudra, who was convicted and sentenced to death for planning the 2002 Bali nightclub bombings in Indonesia, urged Muslims to engage in cyber jihad against U.S. computer systems. Samudra particularly encouraged credit card fraud and provided a primer on how to commit cyber crimes in his recently published memoirs. See Alan Sipress, “An Indonesian's Prison Memoir Takes Holy War Into Cyberspace,” *The Washington Post*, December 14, 2004, <http://www.washingtonpost.com/wp-dyn/articles/A62095-2004Dec13.html> (accessed July 2006).

Weak links in the global information infrastructure. Potentially, any market with a combination of high capacity PCs, broadband connections, and poor network security (typical of most home computers with permanent Internet connections) can be used to wreak havoc on ICT-dependent infrastructure anywhere on the globe via the Internet backbone.⁹ Such weak links create significant vulnerabilities in inadequately protected country networks that are, unfortunately, prevalent in many developing nations. Such networks include both low-bandwidth and very high-capacity networks.

Hacker-activists. Activists and protestors have proven themselves capable of temporarily disrupting ICT-based services of governments and international organizations.¹⁰

Potential military operations. The potential significance of ICT-based services as a part of military “information operations” has been recognized in military and national security doctrines for at least a decade. For example, hostile cyber actions have taken place in the past between India and Pakistan, Azerbaijan and Armenia, and Japan and the People’s Republic of China.¹¹

Rapid evolution of information and communication technologies. Changing technological developments, such as Internet protocol (IP) technology, are radically changing the way that backbone telecommunications services are provided. The increased interdependence between providers of backbone services and providers of services dependent on this backbone creates multiple entry points for network security breaches. Similarly, peer-to-peer technologies that allow millions of end-users to become service providers (e.g., by sharing music and other files) create similar opportunities for security breaches.

A NETWORK MODEL FOR CYBER SECURITY

A well-balanced cyber security policy framework is highly complex. Such a policy framework has no bounds or limits—geographical or jurisdictional. It necessarily encompasses a full spectrum of business, societal, and governmental interests. Although cyber security policy will inevitably address grave concerns about national and global security, as well as well-organized criminal activity, it is fundamentally about creating the very underpinnings of stable economic growth and open, transparent, just, and vibrant societies.

⁹ For instance, there is growing alarm about coordinated efforts to take over and embed in computers—both those owned and operated by individuals and organizations—an unauthorized remote control capacity known as BOTs, which can turn computers into vehicles for attacking and disabling computer networks, network components, and international organizations. This risk grows commensurately as more high-power PCs are connected to the Internet at ever-higher speeds of connectivity.

¹⁰ See Dorothy E. Denning, “Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy” at Totse.com, a Web-based bulletin board that posts information and hosts discussions on a variety of topics, http://www.totse.com/en/technology/cyberspace_the_new_frontier/cyberspc.html, and “Hacktivism: An Emerging Threat to Diplomacy” at the American Foreign Service Association website, <http://www.afsa.org/fsj/sept00/Denning.cfm> (both accessed July 2006).

¹¹ See Charles Billo and Welton Chang, “Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States,” Institute for Security Technology Studies, Dartmouth College, December 2004, <http://www.ists.dartmouth.edu/directors-office/cyberwarfare.pdf> (accessed July 2006).

A “network model”—essentially, a communications network—illustrates how actors in the public and private sectors can work together to manage future cyber risks. Rather than focus on institutions and functions, the focus is on processes, procedures, and information flows within these sectors. In other words, the framework promotes thinking in terms of functions, rather than titles or national or international institutions.

The focus on information flows is intended to help policymakers and other stakeholders visualize the systemic, inter-related nature of cyber security and how the actions of individual entities are likely to impact the decisions and responses of other participants in the network. It should be noted that such a model may require significant changes in traditional roles of intelligence and (inter)national security agencies, requiring them to operate on a more collaborative, inter-institutional basis.

The network model is based on three types of nodes or groups of stakeholders (policymakers, policy implementers, and operational personnel), which exchange three types of information on cyber-security: assessments, responses, and policy. Information exchange occurs both among the nodes, as well as between individual nodes and their peers in outside organizations at all levels.

The model operates in the same way at four different levels, as risk management generally has the same components, regardless of whether it is conducted at the level of a firm, industrial sector, nation, or international organization. First, it requires communications across “organizational” boundaries. Second, it requires information exchange between stakeholders at different levels in the same organization and with other organizations regarding threats that have been encountered and handled. Third, procedures for handling such incidents are required and, fourth, legal or law enforcement sanctions may need to be applied.

At the national level, the major network “nodes” are central coordinating bodies, telecommunications regulators and e-economy ministries, intelligence agencies, law enforcement bodies, and national and governmental Computer Emergency Response Teams (CERTs) and Information Sharing and Analysis Centers (ISACs).¹²

The model works at the international level, where the top-level node is comprised of multinational firms, political and military alliances, which coordinate with such international bodies as the ITU, G8, and the United Nations and its specialized agencies. The implementation node in the international model is comprised of individual national ministries (telecommunications, intelligence, e-economy, and defense ministries, together with law enforcement bodies) and the operational level of national firms (including software and hardware vendors), CERTs, and national defense organizations.

¹² CERTs are teams of ICT professionals who prepare for, and respond to cyber incidents. Typically, they are created within an organization to serve its specific cyber-security needs. An ISAC is a body that allows multiple organizations within a given sector to exchange information. ISACs can belong to the private sector and communicate with the public sector. Governments also establish ISACs. The U.S. Department of Homeland Security, for example, has established several ISACs to facilitate information sharing and network protection in critical infrastructure sectors. See websites of ISACs devoted to financial services (<http://www.fsisc.com>); telecommunication (<http://www.ncs.gov/ncc>); and electric power systems (<http://www.esisac.com>). All sites accessed July 2006.

The drivers of various information exchanges—the factors that shape and influence critical flows of information—include regulatory requirements, liability obligations, and market signals (e.g., risk-related information through which the performance of a network may be influenced). Each national networked relationship may operate with its own unique set of additional drivers. Policymakers may further shape certain drivers to influence node behavior and performance. It may be possible, for example, to strengthen the influence of market-related drivers by using government procurement policies. Insurance and rating companies may use liability strategies to influence the cost of capital and the incentives for security-related investments.

FUNCTIONS OF THE NETWORK MODEL

The goal of the above illustrations is not to describe in definitive terms how these systems should operate. Rather, they are intended to establish a framework for understanding the dynamics of potential cyber security networks, the major functions of which are to:

- Prevent debilitating damage to critical information infrastructures and minimize the risk of cyber attacks.
- Develop mechanisms to respond to cyber incidents.¹³
- Develop effective tools against cyber attacks.
- Assess potential threats.
- Assess the vulnerabilities of critical information infrastructures.
- Improve information security risk management in the public and private sectors.
- Improve information sharing within and between key stakeholders in public- and private-sector entities.
- Improve regulatory tools and mechanisms to minimize cyber risks.
- Develop effective law enforcement tools to analyze hacking incidents and systems (inforensics), as well as to impose penalties and sanctions.
- Improve the security of system and application software.
- Conduct outreach to all key stakeholders.
- Organize effective international coordination among public- and private-sector entities.
- Monitor the performance of cyber-security initiatives.

A brief discussion of the most important of these functions follows. Longer companion papers to this brief policy note address the specific actions that are needed to implement the model at national and international levels.¹⁴

¹³ A cyber security incident first requires the detection of an anomaly or known threat “fingerprint.” Such alarms, after sequencing and correlation, may generate an incident that must be analyzed and acted on. Depending on the determination, if feasible, of the intent of an incident, one may then decide that the incident is a deliberate action, allowing it to be classified as a cyber attack.

¹⁴ See companion papers by the authors of this article (footnote 1): “The Imperatives of National Cyber Security” and “Cyber Security in the International Context,” Global ICT Department of the World Bank, 2005.

Develop mechanisms to respond to cyber incidents. Organizational forms have been developed at multiple levels to investigate, analyze, and respond to cyber-security incidents. CERTs, for example, are becoming the critical backbone for preparing for and responding to cyber incidents of all types. These bodies differ in size and geographic scope and are in varying stages of development in industrialized and developing economies. To date, they are most developed in the financial services and public utilities sectors.¹⁵ Because CERTs are critical hubs for many types of information flows involving a wide range of incidents and different participants, it is critical that they engage in effective collaboration with their counterparts worldwide and develop procedures for managing incidents with a significant international dimension.

Improving risk management and threat assessment. Effective cyber security will depend on strengthening and reinforcing the mechanisms of risk assessment and management within and among companies, organizations, government departments and agencies. Significant threat indicators are likely to emerge only by accumulating, correlating, and analyzing incident-related data at the enterprise level or by analyzing information collected by a range of Computer Security Incident Response Teams (CSIRTs) in multiple countries.¹⁶ “Bottom-up” initiatives are thus the bedrock of cyber-security policy and policymakers will accordingly need to focus on how to support and energize increasingly effective ICT corporate risk management rather than “drive” policy and risk management programs on a top-down basis.¹⁷

Governments are primarily interested in addressing vulnerabilities that would cause a level of harm that does not affect an individual firm, but whose effects would threaten the ability of an entire infrastructure to deliver critical services and goods to the population. From a public policy standpoint, it would thus be constructive to raise the profile of cyber-security risks in the context of the provision of core services.

The key question is whether any rational firm can be expected to invest against hypothetical risks. If threats do not appear tangible, credible or imminent, it will be difficult to mobilize substantial public or private resources in response to them. Although the damage inflicted by network viruses and worms is well documented, it is more difficult to document potential threats from organized criminal elements, hacker-activists, terrorists, or even nation states.

¹⁵ See Myriam Dunn and Isabelle Wigert, “The Critical Information Infrastructure Prevention (CIIP) Handbook 2004”, edited by Andreas Wenger and Jan Metzger (Swiss Federal Institute of Technology), http://www.isn.ethz.ch/crn/docs/CIIP_Handbook_2004_web.pdf (accessed July 2006) for an inventory and analysis of protection policies in 14 countries.

¹⁶ One example of threat identification is the Norwegian experiment with an early-warning system called VDI. See Norway report on the EU Dependability Development Support Initiative (DDSI) website, http://www.ddsi.org/Documents/final%20docs/DDSI_Country_Reports_Final_Norway.pdf (accessed July 2006).

¹⁷ In countries with a long tradition of state involvement or ownership in key infrastructure sectors, such as France, for example, government officials are likely to take a much more top-down, state-directed approach to cyber security, which may inhibit them from entrusting responsibility for risk assessment to corporate executives. In contrast, the Indian Ministry of IT and CERT-In appear to attach high priority to improving risk management at the enterprise level. See various policy presentations prepared for the “Cert-In Workshop on Information Security Policies and Procedures,” New Delhi, September 3, 2004, <http://www.cert-in.org.in/knowledgebase/presentation> (accessed July 2006). The presentations focus on enterprise security architectures and risk management policies.

Decision makers, especially in the private sector, often dismiss threat assessment in favor of evaluating and improving known vulnerabilities. Corporate executives require a well-supported factual and theoretical basis on which to allocate risk-management-related resources. The need to share credible intelligence with senior private-sector decisionmakers will mean that governments must address delicate questions of how and when such sensitive data should be delivered to private-sector participants in a cyber-security network.

There are a number of ways to improve risk management information flows in private firms. One obvious step is to elevate the corporate level at which risk is evaluated to senior executives and the Board of Directors. Another step is to require additional documentation or substantiation with respect to such risk analyses, as well as informal information sharing with peer firms. Such inter-firm communications may, however, require specific authorizing legislation due to existing legal, competitive, and commercial constraints. Corporate cyber risk information should also be gathered from a range of supplier-related sources.

Certain market pressures against risk adverse management can be mitigated if government policymakers effectively make the case that additional security-related initiatives are a matter of overriding public concern. In fact, cyber-security concerns, like quality-of-service issues of an earlier era, must increasingly be viewed as an integral aspect of a product or service, rather than as a separate matter of regulatory concern (i.e., built into a product, not “bolted on” after it is sold and installed).

Assessing the vulnerabilities of critical information infrastructure. The electronic security needs of the financial services sector has already been examined in depth by the World Bank.¹⁸ Other critical sectors that require such assessments include telecommunications (fixed, mobile, satellite, and broadcast); electrical power and utilities;¹⁹ transportation (air, rail, road, sea, river, pipelines); government (e.g., e-government, justice, administration, law enforcement, social services); emergency services, and basic needs (e.g., drinking water, health services).²⁰

Improve information sharing. It is critical that policymakers determine how and what types of information flows are involved in risk management schemes. Creating tools and mechanisms such as cyber-security “exercises” at various levels (public ministry, national and international) would allow governments and the private sector to improve their mutual understanding of the information flows critical to responding to cyber threats and incidents.

¹⁸ The World Bank has established a web portal that includes a wealth of resources and links to financial e-security issues that can be accessed from its Financial Sector Network homepage, <http://www.worldbank.org/finance> (accessed July 2006).

¹⁹ Specifically, such assessments need to address heightened concerns about ICT-control and monitoring systems, or so-called supervisory control and data acquisition (SCADA) systems for electrical power, gas, oil, sewage, and drinking water infrastructure.

²⁰ See the discussion in Dunn and Wigert, “CIIP Handbook”, 2004. Also see H.A.M. Luijff, H.H. Burger, and M.H.A. Klaver, “Bescherming Vitale Infrastructuur: Quick-scan naar vitale producten en diensten – managementdeel (Critical infrastructure protection: Quick-scan of critical products and services; Management report)” TNO Report FEL-03-C001, TNO Information and Communication Technology, The Netherlands, 2003.

Improve regulatory tools. Telecommunications regulators, even in countries where independent regulators have only recently been established, must be prepared to: (1) identify and disseminate “good practices” for dealing with new cyber risks; (2) advise the private and public sectors (including international and national chambers of commerce) on the network protection challenges of new technological developments and the urgent need to implement security measures;²¹ and (3) integrate telecommunications, global grid, and Internet-backbone security concerns into the larger national cyber-security framework.

Develop effective law enforcement tools. Law enforcement bodies need to develop sophisticated forensic techniques for investigating cyber incidents and begin tracking cyber crimes on a long-term basis. Many countries may need to update their legal frameworks in order to address damages to non-physical assets and levy penalties to deter cyber crime.

Coordinate cyber-security initiatives. Oversight of a cyber-security program is a highly complex task. Among the core coordinating tasks in cyber-security framework is establishing the right “neural paths” in the network. This is especially important in the international arena, where collaborative relationships are not yet fully developed. The coordination task will generally require a high-level mandate, as is the case with UK’s National Infrastructure Security Coordination Centre (NISCC)²² and the U.S. Department of Homeland Security.

Develop new international initiatives. Many senior international policymakers are convinced that a new multi-tiered international framework is needed to deal with future cyber threats. This effort would mirror in important respects international collaborative arrangements among intelligence and national security agencies put in place in the context of the Cold War. However, the challenges in responding to a new generation of cyber risks are more complex and require novel cross-border cooperation among governments, NGOs and private-sector entities (including research institutes). ISACs and the larger CSIRT organizations around the globe will, for example, need to share more information on threats and vulnerabilities, as well as improve their capabilities to respond to cyber incidents. One pressing priority is to involve the many developing countries that are not yet considering issues of cyber security in the ongoing international dialogue on the issue.

CONCLUSION

Cyber security is essentially about managing future risk and responding to current and past incidents and attacks. This article has offered a highly decentralized communications model for processing risk-management information about critical information infrastructures, one that can be applied at both the international and national levels. The urgent task ahead is to identify the key information flows that are required for cyber security and to establish linkages among the various organizational entities that can best collect and use this information.

²¹ Rapidly changing technological architectures and new industry structures are likely to affect the basic security of other critical industry sectors as they become increasingly dependent on ICT.

²² The role and functions of the NISCC can be found on its website, <http://www.niscc.gov.uk> (accessed July 2006).