

Document: CNI/04 20 May 2002

Seoul, Republic of Korea — 20 - 22 May 2002

INTERNATIONAL COORDINATION TO INCREASE THE SECURITY OF CRITICAL NETWORK **INFRASTRUCTURES**

This paper was prepared by Seymour E. Goodman, Pamela B. Hassebroek, Davis King and Andy Ozment of the Georgia Institute of Technology, Atlanta, GA, United States, 30332-0610, for the Workshop on Creating Trust in Critical Network Infrastructures, held in Seoul, Republic of Korea, from 20 to 22 May 2002. The workshop was organized by the Strategy and Policy Unit (SPU) of the International Telecommunication Union (ITU), in the framework of the ITU New Initiatives Programme.

The views expressed in this paper are those of the authors and do not necessarily reflect those of ITU or its membership.

ABSTRACT: "[A]ll our infrastructures are increasingly dependent on information and communications systems that criss-cross the nation and span the globe. That dependence is the source of rising vulnerabilities..." Improving the security of these infrastructures requires coordination within and among organizations and nations. With a primary focus on international efforts, we examine the advantages of four forms of cooperation: informal bilateral, formal bilateral, informal multilateral, and formal multilateral. We then consider five areas that demonstrate the value of international coordination: standardization, information sharing, halting attacks in progress, legal coordination, and providing aid to developing nations. To secure these infrastructures effectively, international approaches should be matched with appropriate national strategies. Information security policy efforts in these and other areas should be mindful of unintended consequences. We highlight examples of such consequences in system effects and policy overlap. Despite these and other challenges, international cooperation is a requirement for increasing the security of critical network infrastructures.

¹President's Commission on Critical Infrastructure Protection. (1997, October). *Critical Foundations: Protecting America's Infrastructures The Report of the President's Commission on Critical Infrastructure Protection* (p. i). (GPO No. 040-000-00699-1). Washington, DC: U.S. Government Printing Office. http://www.info-sec.com/pccip/pccip2/report_index.html [2002, April 18].

TABLE OF CONTENTS

1	Introduction5				
	1.1	Threat	ts to security	5	
	1.2	The need for international cooperation			
2	The	The nature of alliance and cooperation.			
	2.1	Informal and formal cooperation			
	2.2	Bilater	ral and multilateral alliances	9	
	2.3	Interna	ational security policy initiatives	10	
3	Opportunities for action				
	3.1	International standards			
		3.1.1	The standardization process	14	
		3.1.2	Standards adoption and compliance	15	
	3.2	Inform	nation sharing: the case for a more effective clearinghouse	17	
		3.2.1	Information dissemination	18	
		3.2.2	Information gathering	18	
	3.3	Haltin	g cyber attacks in progress	21	
		3.3.1	Automated tracing	21	
		3.3.2	Cooperation and coordination with infrastructure operators	22	
	3.4	Coord	linating legal systems	23	
		3.4.1	Harmonization of laws	23	
		3.4.2	Investigation procedures	25	
	3.5	Provid	ding assistance to developing nations	26	
4	Unintended consequences, national strategies, and topical concerns				
	4.1	Uninte	ended consequences of system effects	28	
		4.1.1	System effects applied to security	28	
		4.1.2	Iterative attack/defence cycle	28	
	4.2	Uninte	ended consequences of policy overlap	29	
		4.2.1	Intellectual property	29	
		4.2.2	Civil rights	30	
	4.3	National strategies and national needs			
		4.3.1	Cost planning	30	
		4.3.2	The private sector and software developers	31	
	4.4	Topica	al concerns	32	
		4.4.1	Cyber-terrorism or cyber protest	32	
		4.4.2	Active defences	32	
5.	Conc	iclusions			
ABE	BBREVIATIONS AND ACRONYMS3				
REF	EREN	CES		39	

1 Introduction

"In a world of intertwined global networks, is there a need for a coordinated, sustained, and institutionalized approach to protecting critical network infrastructures?"²

We propose that the answer to this question is yes, and that there is a need not for one, but for several such "coordinated, sustained, and institutionalized" approaches. Both critical network infrastructures and the attacks that threaten them take a wide range of forms; they both also cross borders in complex and sometimes surprising ways. Software written in India controls emergency gas leak repairs in Britain;³ an e-mail from Kenya might cross the Atlantic in route to South Africa;⁴ and a hacker operating from an unidentified country might use computers in Latvia and the United States to attack a South Korean government site.⁵ No single national or international approach can create trust in so many different infrastructure systems.

The International Telecommunication Union (ITU) website further comments, "defenders need to defend against all possible attacks, while an attacker only needs to find a single exploitable weakness." As the builders of the Titanic and the Maginot line found, it is dangerous to assume that any one defence can address "all possible attacks."

We believe, therefore, that the best way to create trust in global networks is to rely not on a single line of defence, but on a series of overlapping defences that include both national and international strategies, public and private efforts, formal and informal channels, and multilateral and bilateral cooperation. The goal of such defences, taken together, should be to help create trust by giving each nation the confidence that when an attack breaches one or more defences, other defences will step into the gap and halt the attack, contain the damage, or deter the attacker from striking again.

In this paper, we focus specifically on opportunities for international cooperation to add to that series of overlapping defences, and on one aspect of trust: security. We do not address other components of trust such as data integrity, software reliability, or engineering standards except as they relate to security, although we anticipate with great interest the discussion of these issues in other papers in this workshop.

1.1 Threats to security

The first factor driving the need for defence is the growing dependence of business and society on critical network infrastructures. Communication has become the lifeblood of modern societies. The rise of e-commerce has made these networks responsible for a growing share of national wealth and hopes for greater prosperity. Furthermore, in some nations, pre-existing critical services have come to rely on electronic networks – emergency services, navigation systems for shipping and air traffic, electric power grids, and water control systems. While these dependencies vary from nation to nation, nearly all nations already or will in the future depend on these critical network infrastructures.

The second factor in the need for defence is that these networks are vulnerable to attack. Many were designed without security in mind, and new vulnerabilities are reported routinely in the most widely used and in even the most recently updated systems. In 2001, for example, the US Computer Emergency Response Team Coordination Center (CERT/CC) received reports of seven new vulnerabilities per day and

²The International Telecommunication Union (ITU) website introduces the New Initiatives workshop on 'Creating Trust in Critical Network Infrastructures' with a series of questions including the one quoted above. From: International Telecommunication Union. (2002, April 12). *Creating Trust In Critical Network Infrastructures*. http://www.itu.int/osg/spu/ni/security/index.html [2002, April 29].

³Wipro, Ltd. *Utilities Case Study #23*. http://www.wipro.com/itservices/industries/utilities/utilicasestudy23.htm [2002, April 30].

⁴BBC News. (2002, April 15). *The great African internet robbery*. http://news.bbc.co.uk/hi/english/world/africa/newsid 1931000/1931120.stm [2002, April 29].

⁵U.S. Senate Permanent Subcommittee on Investigations. (1999, June 5). *Security in Cyberspace* (Appendix B). http://www.fas.org/irp/congress/1996 hr/s960605b.htm [2002, April 30].

⁶International Telecommunication Union. Creating Trust In Critical Network Infrastructures.

published 326 new notes on the most important threats.⁷ It is also well documented that attackers ranging from teenage pranksters to international crime rings have the skills and the willingness to exploit these vulnerabilities for nefarious ends. Of the companies responding to the 2002 CSI/FBI Computer Crime and Security Survey,⁸

- 90 per cent found security breaches;
- 74 per cent were attacked through their Internet connections;
- 85 per cent detected computer viruses.

1.2 The need for international cooperation

One reason for our focus on international cooperation is the sheer difficulty and cost of responding to these threats. Most of the over 200 national and territorial governments of the world are technically or otherwise incapable of dealing with cyber threats on their own. Furthermore, the difficulty of guaranteeing the security of any system requires even the most technically advanced nations to consider costs and benefits carefully in choosing strategies for cyber defence. International cooperation can reduce these costs and increase the range of strategic options that each nation can afford to consider.

A stronger reason is that both the networks and the attackers operate across international borders. "Because all of cyberspace comes to ground somewhere, it has essentially created 'borders' between every pair of countries, and not just those that are physically adjacent." Cooperation is the only way to reduce to manageable levels the resulting combinatorial explosion in numbers of potential attacks and cross-border investigations. Some specific defence strategies, such as shutting down attacking systems and locating and extraditing attackers, may be impossible both technically and legally in the absence of international agreements.

Creating such international agreements is not easy even with a strong consensus in favour of cooperation. In addition to the difficulties of coordinating different governments, cyber defence often requires the involvement of private sector software vendors and infrastructure owners, multiple regulatory and law enforcement bodies from the same State, and different non-governmental organizations with overlapping responsibilities.

We review existing alliances and some of the different alliance structures that defenders may consider in Section 2. In Section 3, we present examples of proposed cooperative measures to illustrate specific areas where we believe international coordination is promising. For each area, we touch upon roles that ITU or other organizations could play, and the tradeoffs between formal/informal and bilateral/multilateral approaches. Finally, in Section 4 we raise some of the difficult questions that any international effort fighting cyber attacks must address.

In all three sections, the topics are not exhaustive. There are many other issues that require careful thought, and many other international approaches that could help to increase security. We hope some of these will be discussed during the workshop.

-

⁷CERT/CC. (2002, April 5). CERT/CC Statistics 1988-2002. http://www.cert.org/stats/cert stats.html [2002, April 29].

⁸Power, Richard. (2002, Spring). 2002 CSI/FBI Computer Crime and Security Survey. *Computer Security Issues & Trends* (p. 4). Computer Security Institute. http://www.gocsi.com/press/20020407.html [2002, April 17].

⁹Goodman, S. E. (2002). Toward a Treaty-Based International Regime on Cyber Crime and Terrorism. In *Transnational Cyber Security Cooperation: Challenges and Solutions* (p. 6). Washington, DC: CSIS Press. Forthcoming.

¹⁰Lukasik, Stephen et al. Strategies for Protecting National Infrastructures Against Cyber Attack. London: International Institute for Strategic Studies. Forthcoming as an Adelphi Paper.

¹¹Goodman, 1.

2 The nature of alliance and cooperation

ITU is a good example of the complex forms that international alliances may take. ITU is both a specialized agency of the United Nations (UN), and a formal, multilateral alliance with private, public, and non-profit members. Its membership includes 189 countries and over 650 groups ranging from regional and international organizations to "the world's largest manufacturers" and "small, innovative new players." Along with its work in establishing telecommunications and radio standards, ITU is also involved in efforts to extend network services in less developed countries. These diverse activities necessitate the diverse organizational forms of its membership.

Forms of international alliance for the protection of critical national infrastructures can be equally complicated. Interactions exist in a variety of modes and serve a variety of purposes, including:

- Sharing information and resources;
- Facilitating discussion;
- Promoting education and awareness;
- Collaborating in research among government, industry and academia;
- Developing international standards;
- Facilitating partnerships between public and private sectors;
- Ensuring public accountability and access to information;
- Acting to support crime prevention, investigation, and prosecution.

This section examines the structure of cooperative efforts, describing alliances according to their degree of formality and the number of parties involved. Using these criteria, we can locate each prospective regime in a four-component matrix, as shown below:

	Informal	Formal
Bilateral	Informal, non-treaty based bilateral coordination	Two-party contractual agreement
Multilateral	Informal, non-treaty based multilateral coordination	Multilateral pact

Forms of inter-party alliance¹³

We use this framework to review existing international security guidelines and agreements in Section 2.3, and to explore areas of further international cooperation in Section 3.

¹²International Telecommunication Union. (2002, April 4). *ITU Membership Overview*. http://www.itu.int/members/index.html [2002, April 30].

¹³Portions of the table taken from: Hamre, John. (Received 2001, December 14). *Memorandum on Trans-national Collaboration in a Cyberage*. CSIS, IDSS, & Markle Foundation.

2.1 Informal and formal cooperation

An informal level of cooperation is most common when two parties have an established relationship and have developed a level of trust that enables them to collaborate on an area of common interest. This trust creates an expectation of confidentiality and reciprocity that facilitates collaboration but does not impose legal obligation. There are no official channels to pursue or particular protocols to follow. Investigations of cyber crime that cross national boundaries frequently rely on informal arrangements.¹⁴

In a formal arrangement the agency or forum is officially established, through an appropriate authoritative channel, with assigned roles and responsibilities for its ongoing operation and maintenance. Specific issues are identified and action procedures are established. Creation of a formal relationship requires a degree of confidence in the other party's ability to fulfill its obligations. All formal international agreements are in writing, often involving a legal instrument, and have a more binding nature than an informal arrangement. The degree of formality may vary from a memorandum that reflects an understanding between representatives of two governments to a treaty that requires ratification by a legislative body.

Each approach, informal or formal, has its benefits in terms of efficiency, scalability, transparency, ease of negotiation, and reliability.

One advantage of informal arrangements is their efficiency in responding quickly to threats—particularly to new or emerging threats. In general, informal efforts use simple communication methods that do not require the navigating of official channels. This efficiency may be crucial when responding to a cyber attack. When an e-commerce website suffers from a denial of service attack, it loses money each second that the site is unavailable to legitimate users.

Formal arrangements enable a cooperative effort to scale more gracefully in size as additional parties are included. The same protocols and official channels that slow their reactions to rapidly emerging threats can make formal arrangements more effective at handling a high volume of requests or operations. For example, a formal agreement can specify the exact procedures necessary for dealing with some varieties of cyber threat

Formal alliances may also be better suited to negotiating cost-sharing and allocating resources in advance for large projects.

In addition, a formal structure may give alliances greater transparency and accountability. Transactions may be recorded, and the authorship of specific decisions may be visible. Informal arrangements, on the other hand, can be opaque – an individual in one organization may simply make a phone call to an individual in a different organization, with no record of the transaction.

Formal arrangements, because they are legally binding, are often more complex to negotiate than informal arrangements. The Council of Europe (COE)'s Convention on Cybercrime is a pertinent example: the creation of this formal agreement required five years of negotiations and numerous draft revisions. Despite this lengthy period of negotiation, the Convention has not yet come into effect. Although 30 countries signed it in November of 2001, the ratification of five signatory countries is still required.¹⁵

The legally binding aspect of a formal arrangement can increase its reliability, however; it gives each party the confidence that the other parties are legally obligated to follow the terms of the agreement. A formal relationship thus creates an expectation of predictable compliance and performance. Because requirements are clearly elucidated in the agreement, the parties are able to plan more effectively and to allocate resources in advance.

¹⁴Vatis, M. (2002). International Cyber Security Cooperation: Informal Bilateral Models. In *Transnational Cyber Security Cooperation: Challenges and Solution* (p. 6). Washington, DC: CSIS Press. Forthcoming.

¹⁵The European Committee on Crime Problems created a subcommittee on cyber-crime in November 1996. This Committee of Experts on Crime in Cyber-space commenced its work in April 1997. The treaty they created was opened for signature on November 11, 2001. From: Council of Europe. (2001). *Convention on Cyber crime ETS no.: 185 – Explanatory Report* (Article II, Section II). http://conventions.coe.int/Treaty/en/Reports/Html/185.htm [2002, April 5].

2.2 Bilateral and multilateral alliances

Cooperative alliances can be broadly characterized as bilateral or multilateral. Regardless of the formality of cooperation, the number of parties involved affects the ease of negotiation, level of cooperation, consistency, resources, and impact of the effort.

Bilateral agreements are often easier to negotiate than multilateral efforts. The greater the number of parties involved in securing an agreement, either formal or informal, the greater is the complexity in negotiation and in cooperation. Increasing the number of parties involved increases complexity due to the diversity of individual agendas. The difficulties in negotiating a multilateral agreement are further compounded if the agreement is also formal, as demonstrated by the lengthy negotiations required to create the COE Convention on Cybercrime. Because of its relative ease of negotiation, a bilateral arrangement can be a useful test bed for determining effective approaches for multilateral cooperation.

Another advantage of bilateral efforts is that States can vary their degree of cooperation in accordance with the degree to which they trust their partner. If the effort involves a trading partner or trusted ally, a country may be far more willing to share resources and information than with a country whose reliability is unknown. This issue of trust can complicate the creation and operation of a multilateral agreement, which must address the tensions and cultural/ideological differences that exist among countries. Multilateral agreements must also consider that some States may not share the mutual security interests of the majority, due to a concern for loss of policy autonomy or an actual adversarial position.¹⁶

Mutual Legal Assistance in Criminal Matters Treaties (MLATs) are a good example of the differentiated levels of cooperation possible under a bilateral regime. The United States has implemented MLATs with nineteen other countries.¹⁷ These formal, bilateral treaties are used in the prosecution of transnational crime and are thus important for cyber crime investigations:

"[MLATs] seek to improve the effectiveness of judicial assistance and to regularize and facilitate its procedures. Each country designates a central authority, generally the two Justice Departments, for direct communication. The treaties include the power to summon witnesses, to compel the production of documents and other real evidence, to issue search warrants, and to serve process. Generally, the remedies offered by the treaties are only available to the prosecutors. The defense must usually proceed with the methods of obtaining evidence in criminal matters under the laws of the host country, which usually involve letters rogatory." ^{18, 19}

Because MLATs are bilateral, they enable the participating parties to enter into agreements selectively with only those States whose legal systems are compatible. In general, agreements can include a greater level of cooperation when the interests of States are highly compatible.

Although less flexible with respect to the level of cooperation, a single multilateral agreement can be more consistent than a patchwork of bilateral agreements. This advantage could have a significant effect on cyber crime investigations, which in many cases must proceed rapidly and may involve a number of States:

¹⁶Vatis, 3-4.

¹⁷Another fifteen treaties are signed but not yet in force.

¹⁸U.S. Department of State. *Mutual Legal Assistance in Criminal Matters Treaties (MLATs) and Other Agreements*. http://www.travel.state.gov/mlat.html [2002, April 5].

¹⁹ Letters rogatory are the customary method of obtaining assistance from abroad in the absence of a treaty or executive agreement. A letter rogatory is a request from a judge in the United States to the judiciary of a foreign country requesting the performance of an act which, if done without the sanction of the foreign court, would constitute a violation of that country's sovereignty. Prosecutors should assume that the process would take a year or more. Letters rogatory are customarily transmitted via the diplomatic channel, a time-consuming means of transmission. The time involved may be shortened by transmitting a copy of the request through Interpol, or through some other more direct route, but even in urgent cases the request may take over a month to execute." From: United States Department of Justice. (1997, October). *United States Attorneys' Manual* (Title 9, Criminal Resource Manual, 275 Letters Rogatory). http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/index.htm [2002, April 4].

different procedures established through a series of bilateral agreements may actually "impede a criminal investigation that is truly multinational in scope." ²⁰

By harnessing a large number of parties, a multilateral agreement can also pool resources and thereby lessen the impact on any single party. This benefit is especially important where there is significant inequity in resources. In the International Organization for Standardization (ISO), for example, States contribute according to a formula that takes into account their gross domestic product. This method ensures that States support the organization without being overly burdensome for developing nations.

Multilateral agreements, particularly those with near-universal participation, can also have a greater impact than bilateral agreements. Civil aviation presents a good example of the value of an international agreement with near-universal participation. A number of international conventions focus on countering hijacking and other crimes against the civil aviation infrastructure. Near-universal membership ensures that those who commit crimes against the civil aviation infrastructure are denied a safe haven. "Since adoption of the civil aviation treaties, sabotage and acts of unlawful interference have steadily declined."²¹

A non-universal multilateral agreement, however, may have externalities. The Internet can be viewed as common property – a public good, open for anyone to use. Whether or not a party contributed to the development of the Internet and the critical network infrastructures upon which it relies, that party can reap both the benefits and the drawbacks of the network's use. This aspect of the infrastructure leads to the free rider problem: parties can use a commodity for which they do not pay. All States will benefit from international efforts to increase the security of critical network infrastructures, whether or not those States are involved in the efforts. In effect, States may be tempted to act as free riders, enjoying the benefits of international efforts without the costs.

2.3 International security policy initiatives

Despite the political and technical complexity of improving security, many international efforts are already making progress. In the interest of space, we limit our review of these precedents to the work of the Organization for Economic Cooperation and Development (OECD), the G-8 Subgroup on High-Tech Crime, the COE Cybercrime Convention, and the Stanford Draft Convention. These examples are not exhaustive: many other active international initiatives, such as those of the UN and the Asia-Pacific Economic Cooperation (APEC), are also worthy of examination.

The OECD Information, Computer and Communications Policy (ICCP) Committee developed the OECD Guidelines for the Security of Information Systems as a model for national policies in member countries. They were developed by a Group of Experts drawn from government, industry, and academia, and were adopted by the OECD member countries on 26 November 1992.²² One of the goals of the work is the protection of individuals and organizations from harm resulting from failures of security.

The OECD security guidelines followed the model of the OECD Guidelines on Privacy, which were developed in 1980. Kirby and Murray report that the privacy guidelines succeeded in influencing laws and policies in OECD countries, and they attribute its success to its non-coercive nature. The OECD's strategy of voluntary compliance allows a member country to use the guidelines to assist in creating domestic security policy. Now that the guidelines have contributed to harmonization of laws in many of these countries, they could make it easier to negotiate formal multilateral cooperation that includes enforceable international law.²³

²⁰Litt, Robert S. and Lederman, Gordon N. (2002). Formal Bilateral Relationships as a Mechanism for Cyber Security. In *Transnational Cyber Security Cooperation: Challenges and Solution* (p. 5). Washington, DC: CSIS Press. Forthcoming.

²¹Cuellar, Mariano-Florentino. The Civil Aviation Analogy. In Abraham Sofaer and Seymour Goodman (Eds.), *The Transnational Dimension of Cyber Crime and Terrorism* (p. 112). Stanford, CA: Hoover Institution Press, 2001.

²²Organization for Economic Cooperation and Development. (1997, July 1). *Guidelines for the Security of Information Systems* (Preface). http://www1.oecd.org/dsti/sti/it/secur/prod/e_secur.htm [24 April 2002].

²³Kirby, M. and Murray, Catherine A. (1993). Information Security: At Risk? In L. M. Harasim (Ed.), *Global Networks: Computers and International Communication* (p. 173). Cambridge, MA and London: The MIT Press.

The security guidelines were developed at a time when Internet use was much less widespread than today. Many security issues related to the Internet and networking, therefore, received less attention in the Guidelines than they would receive in a similar security policy written today. These issues are not entirely new, but they gain significance as increasing connectivity multiplies and diversifies both the threats information systems face and the potential consequences of those threats.

A survey of OECD members in 1997 indicated that the Guidelines still provide valuable structure to information systems security issues, even with their limitations for addressing today's threats.²⁴ Currently, some organizations are using the OECD guidelines as a focus in collaborative sessions regarding cyber crime.^{25, 26} The survey indicated that members believe the OECD is placed ideally to act as a forum for discussion, debate, and the exchange of information. Members also suggest that the OECD could be used to test the relevance of security principles before they are made directly applicable or deemed binding within another framework.²⁷

The G-8 Subgroup on High Tech Crime is another example of international cooperation to increase network security. This informal, multilateral, (but not universal) effort was formed in January of 1997 and has since been expanded to include a number of non-G-8 countries. The G-8 Subgroup has focused its work in four different areas: communication, training, legal systems coordination, and industry/law enforcement collaboration. It has had noteworthy success in fostering speedy communications between countries to enable preservation of digital evidence for formal legal proceedings.²⁸

Via meetings with law enforcement and industry representatives, the Subgroup has developed concrete steps that can be taken to improve cooperation between these two sectors to allow industry to respond to incidents more quickly and with less expense. They have developed a checklist of standard procedures for preserving evidence, for tracing communications in real-time, and for authenticating users.²⁹ Such information can assist in locating attackers, halting the advance of an attack, and preventing further damage and attack recurrence.

While limited in membership, the G-8 has served as a model for multilateral efforts. It has fostered informal cooperation between law enforcement agencies from different States, and helped identify important issues for international cooperation with respect to network security.³⁰ Nonetheless, its lack of universal coverage and uniform process has led many to advocate a more formal multilateral effort.

Both the COE Cybercrime Convention³¹ and the Stanford Draft Convention^{32, 33, 34} are attempts to meet this need. However, unlike the COE Cybercrime Convention, the Stanford Draft Convention is an academic proposal that does not yet have official sponsorship.

²⁹Vatis, 5.

²⁴Organization for Economic Cooperation and Development. (1997). Review of 1992 OECD Guidelines for the Security of Information Systems. http://www1.oecd.org/dsti/sti/it/secur/prod/reg97-2.htm [2002, May 10].

²⁵Ministry of Economy, Trade, and Industry. (2001, September 3). *OECD Workshop: "Information Security in a Networked World"*. http://www.meti.go.jp/policy/netsecurity/OECDwrkshpAgenda.htm [2002, May 11].

²⁶Federal Trade Commission. *Public Workshop: Consumer Information Security*. http://www.ftc.gov/os/2002/03/frncis.htm [2002, May 11].

²⁷Organization for Economic Cooperation and Development, *Review of 1992 OECD Guidelines for the Security of Information Systems*.

²⁸Vatis, 5.

³⁰Vatis, 5-6.

³¹More information on the Cybercrime Convention (ETS no. 185), including the text, is available at: http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185

³²Sofaer, Grove, and Wilson. (2001). Draft International Convention to Enhance Protection from Cyber Crime and Terrorism. In A. D. Sofaer, and Seymour E. Goodman (Ed.), *The Transnational Dimension of Cyber Crimes and Terrorism*: The Hoover Institution on War, Revolution and Peace.

The COE Convention was drafted for the purpose of mutual legal assistance. Its purpose is to achieve a harmonization of substantive criminal laws, establishment of procedural laws, and a system for the provision of assistance to other States. As described later in this paper, all of these goals are important steps necessary to effectively combat cyber crime. Henrik Kaspersen argues that the COE agreement "should have its place amid other kinds of initiatives in international cooperation, both formal and informal, to shape an effective approach to the prevention and repression of cyber crimes."³⁵

However, the COE Convention has been the subject of criticism as well as of praise. Much of this criticism focuses on the provisions regarding content legislation (child pornography and intellectual property), the significant attention to focus on procedural laws, and on the duties imposed on private infrastructure operators.

The Stanford Draft Treaty attempts to avoid these pitfalls. It focuses on:

- crimes against systems and networks;
- harmonization of laws;
- near-universal participation;
- providing assistance to developing nations;
- protecting human rights;
- avoiding technical or procedural detail that may become outdated;
- avoiding restrictions on the actions of States in regards to information warfare.³⁶

In doing so, it avoids the controversial content-related points and the possibly restrictive procedural detail that have created concern about the COE Convention. In addition, the Stanford Draft Convention would create a new organization, the Agency for Information Infrastructure Protection (AIIP), to coordinate efforts to reduce cyber crime and to provide assistance to developing countries so that they can fulfill their obligations under the treaty. The Stanford Draft does nevertheless leave many unanswered questions: how will States be sanctioned when they fail to fulfill their duties? How will the AIIP be funded? How will public/private sector interaction work? How will near-universal participation be achieved? How will non-signatories be treated? Similarly though, the COE Convention fails to address many of these points.^{37, 38}

Whether a formal, multilateral agreement is achieved through the COE Convention, the Stanford Draft Convention, or some other instrument, such an agreement is important for enabling law enforcement officials to effect investigations that must involve multiple States. Without an agreement, variations in security standards and legal systems may risk creating havens for criminals. "Near-universal participation makes the problem legitimate globally, and tries to eliminate safe havens." As in civil aviation, the elimination of safe havens for attackers can have a significant deterrence affect.

³³Goodman

³⁴Sofaer, Abraham D. and Goodman, Seymour E. (2000, August). A Proposal for an International Convention on Cyber Crime and Terrorism. The Hoover Institution: Stanford, CA

³⁵Kaspersen, Henrik. A Gate Must Either Be Open or Shut: The Council of Europe Cybercrime Convention Model. In *Transnational Cyber Security Cooperation: Challenges and Solutions* (p. 12). Washington, DC: CSIS Press. Forthcoming.

³⁶Goodman, 6-7. Much of the other information in this paragraph was also taken from this source.

³⁷Goodman, 8-9.

³⁸For a more detailed analysis of the COE Convention and the Stanford Draft Treaty, see: Lukasik, Stephen. (2001, October). *Responding to Cyber Threats: The International Dimension*. Stanford University's Consortium for Research on Information Security and Policy & the Georgia Tech Information Security Center.

³⁹Goodman, 6.

3 Opportunities for action

While it is unlikely that a single, universal, international agreement for increasing network security is achievable, it is desirable to work toward consensus in some critical areas. In this section, we focus on five opportunities for cooperation that we believe impact the overall security posture of critical network infrastructures: international standards, information sharing, halting attacks in progress, coordinating legal systems and providing assistance to developing countries. For each area, we examine current international efforts and suggest where new or expanded efforts could be beneficial.

3.1 International standards

Every electronic network in existence depends on the ability of different components on the network to interpret a given electronic signal in a consistent way. Standards are what make this possible, and as a result, the security of any network depends directly on the underlying security of its standards. If a standard specifies an encryption algorithm later found to be insecure, if it requires passwords or other critical data to be sent in a readable format, or if it makes it too difficult to distinguish legitimate data from malicious data, it can render an entire network insecure.

All of these flaws are exhibited in the standards currently in use. For example, both the Content Scrambling System (CSS) encryption used to prevent DVDs from being copied and the WEP security protocol used to protect IEEE 802.11 wireless networks employ encryption algorithms that are easy to break.^{40, 41, 42} Several standard Internet services, such as the Telnet protocol, send passwords as plain text that hackers can read with sniffer programs. And, as discussed in Section 3.3.1 below, the IP protocol itself does not offer efficient means of tracing malicious packets back to their source.

Even standards without intrinsic flaws can contribute to insecurity if vendors make mistakes in standards compliance or when servers use obsolete protocols. For example, some significant flaws in Microsoft's Internet Information Server are related to failures to handle invalid Unicode data properly, and many security holes in Unix systems are related to bugs in obsolete versions of SSH, BIND, and other programs used to comply with Internet standards.⁴³

To understand this problem clearly, we must define more precisely what we mean by standard. Even in the limited setting of electronic networks, the word "standard" can be used in many different ways. In the case of ITU standards, or "recommendations" produced by the Telecommunication Standardization Sector (ITU-T), for example, to gain official status as an ITU-T Recommendation a draft must pass through a rigorous public approval process that gives 189 national governments and many other organizations opportunities to comment. Recommendations with policy or regulatory implications cannot be approved if 30 per cent or more of the comments received from Member States are negative. Each of ITU-T's 2,800 Recommendations currently in force, therefore, can be called an official standard in the sense that it has been thoroughly examined and approved by an organization with 130 years experience and the backing of the UN. 44, 45

⁴⁰Schneier, Bruce. (2001, August 13). *Declaration of Bruce Schneier in Felten v. RIAA*. Electronic Frontier Foundation. http://www.eff.org/IP/DMCA/Felten_v_RIAA/20010813_schneier_decl.html [2002, May 6].

⁴¹Gast, Matthew. (2002, April 19). *Wireless LAN Security: A Short History*. O'Reilly Network. http://www.oreillynet.com/pub/a/wireless/2002/04/19/security.html [2002, May 6].

⁴²Arbaugh, William A. et al. (2001, March 30). *Your 802.11 Wireless Network has No Clothes*. http://www.cs.umd.edu/~waa/wireless.pdf [2002, May 6].

⁴³Internet Security Systems. (2000, October 26). Serious flaw in Microsoft IIS Unicode translation http://www.iss.net/security_center/alerts/advise68.php [2002, May 6].

⁴⁴International Telecommunication Union Technology Telecom Standardization (ITU-T). (2000, October). *Alternative Approval Process for New and Revised Recommendations*. (ITU-T Recommendation A-8). http://www.itu.int/dms_pub/itu-t/rec/a/T-REC-A.8-200010-I!!PDF-E.pdf [2002, May 6].

⁴⁵ International Telecommunication Union. *ITU Overview – World Telecommunication Standardization Assembly*. http://www.itu.int/aboutitu/overview/wtsa.html [2002, May 6].

The computer data flowing over lines built to ITU standards, meanwhile, may follow "standards" proclaimed by private companies, governments, organizations (such as the World Wide Web Consortium (W3C)) that have no official status, or by a wide variety of other official and semi-official standards bodies. One influential standards-setting body, the Internet Engineering Task Force (IETF), defines "standard" as follows:

"In general, an Internet Standard is a specification that is stable and well-understood, is technically competent, has multiple, independent, and interoperable implementations with substantial operational experience, enjoys significant public support, and is recognizably useful in some or all parts of the Internet."

Their definition does not mention either the legal status or the universality of a potential standard, and it allows multiple competing specifications for the same application to be referred to as standards. One IETF member described their approach as "We do not worry about presidents and kings; we work by rough consensus and running code." The IETF's structure is also unusual for a standards body:

"The Internet Engineering Task Force is a loosely self-organized group of people who contribute to the engineering and evolution of Internet technologies... The IETF is unusual in that it exists as a collection of happenings, but is not a corporation and has no board of directors, no members, and no dues." 48

In spite of their vastly different legal status and approach to defining standards, the IETF and ITU collaborate and have even developed standards jointly in areas of mutual interest.⁴⁹ As a unit of the Internet Society (ISOC), the IETF is considered part of an ITU Sector Member, and the two organizations have official procedures in place to comment on each other's proposals.

We will use the IETF's definition of standards when referring to Internet standards or other standards developed via the IETF's 'Request for Comments' (RFC) process. In certain cases, we will also refer to widely used standards developed by a single company and available in only one implementation as "proprietary standards." While these single-company specifications are not standards in the strict legal sense, they are subject to many of the same security risks. Intel's x86 assembly instructions and the Windows API's used by all software programs running on Microsoft Windows are examples of such proprietary standards.

3.1.1 The standardization process

One reason why standards are difficult to make secure is that many different organizations, vendors, and even individuals can propose new standards. These contributors may differ in both the level of attention they are currently giving to security and in when they chose to make a security a primary design criterion. At one extreme, the Japanese Government Ministry for International Trade and Industry (MITI), produced its first computer systems security standards in 1977. At another, in 2002 Microsoft Corporation declared as a new strategic goal "Trustworthy Computing" – "computing that is as available, reliable and secure as electricity, water services and telephony." Other standards drawn up in the 1980s and 1990s run the gamut from making security a priority to ignoring it completely.

⁴⁶Bradner, Scott. (1996, October). *The Internet Standards Process – Revision 3*. Request for Comments 2026, Network Working Group, IETF. http://www.ietf.org/rfc/rfc2026.txt [2002, May 11].

⁴⁷David Clark, quoted in Baker, Fred. (2000, January 25-27). *Internet Standardization and the IETF* (slide 24). IP-Telecoms Interworking Workshop (Numbering, Naming, and Routing), ITU, Geneva. http://www.itu.int/ITU-T/worksem/ip-telecoms/presentations/ipw-7.ppt [2002, May 11].

⁴⁸Harris, Susan (Ed.). (2001, August). *The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force*. (Internet Engineering Task Force RFC 3160). http://www.ietf.org/tao.html [2002, April 18].

⁴⁹Richenaker, Gary. (2001, December 18). *Report of IP-Telecoms Interworking Workshop (Numbering, Naming, Addressing and Routing) ITU, Geneva 25-27 January 2000.* http://www.itu.int/ITU-T/worksem/ip-telecoms/index.html

⁵⁰Gates, Bill. (2002, January 17). Trustworthy Computing. *Wired.com*. http://www.wired.com/news/business/0,1367,49826,00.html [2002, April 28].

An example of the change in the standardization process over time is the IETF's Simple Network Management Protocol (SNMP). Introduced in the late 1980s to control network devices from routers to manufacturing and medical equipment, SNMP is still in use as "the most popular protocol in use to manage networked devices." However, the original SNMP proposals never even mention security. Perhaps as a result of this, SNMP and its implementations have been plagued with difficult-to-repair vulnerabilities. Planning is currently under way for a replacement, SNMPv3. Not surprisingly, the new version includes Internet Drafts for several different security systems designed to work with SNMPv3, and the primary draft for the complete system includes security and access control among its highest goals. 54,55

Another major difference among the practices of different standards-setting groups is their approach to openness and vulnerability disclosure. Schneier attributes the weakness of the WEP and DVD encryption methods to a development process that attempted to keep the algorithm details secret instead of allowing security experts to test the protocols via peer review.⁵⁶ Debates are also frequent over whether the best approach to correct vulnerabilities in standards and vendor implementations is to release information promptly to the public, to the vendor only, or to both at different times. Christey and Wysopal made a thus far unsuccessful attempt to create a standard for "responsible disclosure" through the IETF.⁵⁷

3.1.2 Standards adoption and compliance

Despite the progress made by the IETF, it faces a challenge in improving the security of Internet Standards⁵⁸ worldwide. The problem is that its standards are largely recommendations, accepted on the basis of "rough consensus and running code" and relying on software vendors, system owners, and other national and international standards bodies to choose which specific standards to support. This is compounded by the fact that many other organizations and software vendors are busy creating alternative standards for their own purposes. For example, the widespread use of Microsoft Windows awards some Microsoft proprietary standards, such as Visual C++ and COM objects, a 'de facto' advantage over ISO/ANSI Standard C++ or CORBA.

Improving the security of standards used in practice will require: (1) encouraging organizations that create standards to address security, and (2) convincing vendors and customers to consider security when they choose competing standards.

Public criticism and market pressure may already be giving some large companies an education in the value of security. Microsoft's Trustworthy Computing initiatives were instigated in the wake of the heavy criticism that Microsoft received when the Code Red and Nimda worms struck Windows systems in 2001.^{59, 60, 61, 62}

⁵¹CERT/CC. (2002, February 13). SNMP FAQ. http://www.cert.org/tech_tips/snmp_faq.html [2002, April 17].

⁵²CERT/CC. (2002, April 16). CERT Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP). http://www.cert.org/advisories/CA-2002-03.html [2002, April 17].

⁵³An 'Internet Draft' is any RFC under IETF consideration as a draft of a proposed future standard.

⁵⁴Harrington, D. et al. (1999, April). *An Architecture for Describing SNMP Management Frameworks*. Request for Comments 2571, Network Working Group, IETF. http://www.ietf.org/rfc/rfc2571.txt?number=2571 [2002, May 11].

⁵⁵Blumenthal, U. and Wijnen, B. (1999, April). *User Based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*. Request for Comments 2574, Network Working Group, IETF. http://www.ietf.org/rfc/rfc2574.txt?number=2574 [2002, May 11].

⁵⁶Schneier, Declaration of Bruce Schneier in Felten v. RIAA

⁵⁷Christey, Steve and Wysopal, Chris. (2002, February). *Internet Draft: Responsible Vulnerability Disclosure*. Internet Engineering Task Force. http://www.ietf.org/internet-drafts/draft-christey-wysopal-vuln-disclosure-00.txt [2002, May 6].

⁵⁸An 'Internet Standard' is any RFC that the IETF has approved as an official standard.

⁵⁹Lemos, Robert. (2002, January 11). Microsoft's security push lacks oomph. *CNET News.com.* http://news.com.com/2100-1001-808010.html [2002, April 28].

Microsoft has since sent large numbers of its programmers to a month-long security training programme, although the results of their effort have yet to be seen. The IT industry has announced similar initiatives in the past, such as the Trusted Computing Platform Alliance announced by Compaq, HP, IBM, Intel, and Microsoft in the autumn of 1999. However, this formal, multilateral effort has released few materials since its first specification draft.⁶³

Insurance companies and legal liabilities provide another mechanism to influence choices among standards. Schneier has argued that exposing software vendors to greater legal liability could be a critical step in getting them to address security. For business customers, insurance companies can use rate reductions as an incentive to encourage purchases of software and hardware designed for security. J.S. Wurzler Underwriting Managers is charging from five to 15 per cent surcharges on its cyber insurance premiums for companies using Microsoft's web server.^{64, 65}

National governments may also be able to affect standards adoption by using both soft power methods such as changing their own purchasing rules and security guidelines, and hard power methods such as tax changes and new regulations. In the United States, for example, the federal Government is the single largest consumer of information technology products. ⁶⁶ Erbschloe writes "[t]he [US] military and the Government don't really have too much choice at this point except to start to put pressure on Microsoft and others to improve software security. ⁶⁷ If the US and other States with substantial purchasing power in the field of information technology required that their purchases meet security standards, they could increase the size of the market for high-security products. ⁶⁸

The MITI security initiative in Japan is an example of an attempt to influence the market in a non-coercive manner similar to the methods used with the OECD Guidelines. The MITI standards, and their subsequent revisions, do not have legal force in Japan, but serve as a basis for systems procurement by government or industry. They were established primarily to motivate action to prevent security breaches.⁶⁹

Japan has further encouraged the private sector to focus on security with tax incentives and favourable financing methods that promote the development of secure systems.⁷⁰

⁶⁰Acohido, Byron. (2002, March 10). Air Force seeks better security from Microsoft. *USA Today*. http://www.usatoday.com/life/cyber/tech/2002/03/11/gilligan.htm [2002, April 28].

⁶¹Wilcox, Joe. (2002, February 12). Can MS juggle privacy and security? *ZDNet News*. http://zdnet.com.com/2100-1104-835802.html [2002, April 28].

⁶²Pescatore, John. (2001, September 19). *Nimda Worm Shows You Can't Always Patch Fast Enough*. Gartner Research. http://www4.gartner.com/DisplayDocument?id=340962&acsFlg=accessBought [2002, April 28].

⁶³Trusted Computing Platform Alliance. http://www.trustedpc.org [24 April, 2002].

⁶⁴Brush, Colleen. (2001, July). Surcharge for Insecurity. *Information Security Magazine*. http://www.infosecuritymag.com/articles/july01/departments news.shtml [2002, April 27].

⁶⁵On the other hand, "I think (Wurzler) did it to make press,' says Russ Cooper, moderator of NTBugtraq and surgeon general of TruSecure Corp. (www.trusecure.com). 'My understanding is that they are desperately looking for business, and this is one of the ways to get it.' "Cited in Brush, Colleen. (2001, July). Surcharge for Insecurity. *Information Security Magazine*. http://www.infosecuritymag.com/articles/july01/departments_news.shtml [2002, April 27].

⁶⁶The Canadian Trade Commissioner Service. (2000). *EXTUS Trade Mission – Globetech – Sector Information – Technology in Washington*. http://www.infoexport.gc.ca/mission/globetech/tech_in_wash-e.asp [2002, May 6].

⁶⁷Cited in Acohido, Byron. (2002, March 10). Air Force seeks better security from Microsoft. *USA Today*. http://www.usatoday.com/life/cyber/tech/2002/03/11/gilligan.htm [2002, April 28].

⁶⁸Litt and Lederman, 7.

⁶⁹Kirby and Murray, 181.

 ⁷⁰ Japan Country Report. (2002). Japan Country Report. In *Transnational Cyber Security Cooperation: Challenges and Solutions* (p. 7). Washington, DC: CSIS Press. Forthcoming.

Regulations were widely used to address the Year 2000 (Y2K) bug, a problem with many of the same implications for trust as insecurity. During the run-up to the beginning of the year 2000, industry mobilized and governments passed laws requiring Y2K certification of technology components. In the US, the Securities & Exchange Commission (SEC) required corporations to report their Y2K compliance efforts in quarterly earnings reports. This regulation provided accountability and achieved a security standard. Similar regulation might help bring market pressure to bear on the vendors of proprietary standards.

No organization, however, can use the methods described in this section to influence standards adoption unless the organization is first aware of the security issues involved. Coordinating the efforts of governments, insurers, and regional and national standards groups might be an interesting area for ITU to explore. ITU's organizational structure provides channels for communication with national standards bodies, private companies, and non-governmental organizations around the world. ITU also has official credibility that may lead some governments to accept security recommendations coming from ITU or from an ITU-recommended source more readily than those coming from a non-UN organization like the IETF.

3.2 Information sharing: the case for a more effective clearinghouse

Improving the standards design process is a long-term solution. To remedy existing vulnerabilities, shorter-term solutions—like information sharing—are necessary. Many information sharing efforts are already under way to inform system administrators about patches, known hacker methods, and other newly discovered security issues.

Unfortunately, the current information sharing regime is ineffectual, as system administrators must monitor an overwhelming number of sources in order to remain aware of potential network vulnerabilities.⁷¹ At the same time, better information gathering would greatly improve the ability of entities to secure their organizations. In particular, it will help solve three key challenges in the protection of network infrastructure: prioritizing defensive measures, obtaining executive support, and risk assessment.

System administrators need a manageable means for acquiring the comprehensive information necessary to put specific vulnerabilities into perspective. Quantitative statistical data concerning the number of network vulnerabilities, the cost of repairing them, and the potential risk of not repairing them could improve administrators' ability to target the most critical threats first.

Statistical data would also help information security practitioners to make a more effective business case for increased attention to security. In many organizations, both public and private, these practitioners struggle to obtain from their upper management the resources and commitment necessary to secure their networks. Unfortunately, in the current environment, their cases are often only heard once a damaging intrusion has actually taken place.

Quantitative statistical data would also improve organizations' ability to assess risk, which would be valuable for both business planning and for the insurance industry. Few insurance companies have offered policies that cover losses incurred by system and network security failures.^{72, 73} Widespread offerings have not been forthcoming because the insurance industry lacks sufficient data to quantify security risks. On those few policies currently offered, premiums may be set unusually high in an attempt to compensate for unknown risk.

Insurance companies may serve more than one purpose in the network security process. While an expanded array of insurance products will assist in risk management, requirements for insurance may actually force companies to increase internal network security, as mentioned in Section 3.1.2. Some security professionals believe that the insurance industry will eventually drive security reforms in the information technology

⁷¹Frequently used sources include the Bugtraq mailing list, CERT/CC, CIAC, vendor specific mailing lists, SANS, SecurityTracker.com, and many other web sites and mailing lists.

⁷²Radcliff, Deborah. (2000, August 21). Got Cyber Insurance? *Computerworld*. http://www.computerworld.com/managementtopics/ebusiness/story/0,10801,48721,00.html [2002, May 7].

⁷³Lai, Eric. (2002, March 14). *Cyber-insurance gaining popularity due to high-tech risks*. MSNBC. Reuters. http://stacks.msnbc.com/local/rtor/m23000.asp?cp1=1 [2002, April 5].

industry⁷⁴ – much like pressure from the insurance industry helped bring about improvements in automobile and building safety.

While there are many organizations with some form of clearinghouse function; at present no international organization is widely recognized as *the repository* of comprehensive information concerning vulnerabilities and attacks. A more effective information clearinghouse could enhance our capabilities in this area; international cooperation could ensure that this clearinghouse is both effective and universally recognized.

3.2.1 Information dissemination

Streamlining the dissemination of information would provide immediate benefits to administrators. A single information clearinghouse would reduce the number of sources that administrators must monitor in order to ensure their awareness of vulnerabilities and to learn how to correct those vulnerabilities. In the current environment, for example, a system administrator might learn about an important vulnerability by monitoring the Bugtraq⁷⁵ mailing list, but the list might not explain how to secure systems that have this vulnerability. That system administrator is then forced to search other resources to find the required information. An information clearinghouse could serve as a single location to collect and disseminate all of the security information available.

In addition to reducing the number of sources, an information clearinghouse could reduce the volume of unwanted information. It could enable system administrators to learn only about vulnerabilities in systems that they administer. In essence, the filtering function would move from the individual system administrator to the clearinghouse. The Cassandra⁷⁶ project at Purdue University is a nascent effort to achieve this goal. System administrators register to receive vulnerability reports for only that software in which they have an interest. Although it is a step in the right direction, the Cassandra project has flaws that hinder its usefulness.⁷⁷ Building on the efforts of the Cassandra project and coupling it with an information clearinghouse could improve the ability of system administrators to effectively secure their systems.

A clearinghouse could also serve as an early warning centre, notifying system administrators of new vulnerabilities as they become apparent. The usefulness of this function may be best illustrated by the life cycle of viruses and worms. Because of the manner in which viruses and worms propagate, warnings could be received from the first affected time zone early enough to enable system administrators in other time zones to successfully defend themselves. This central source would increase both the speed with which information could be disseminated and its likelihood of reaching the target audience. Recognizing this, Belgium last year advocated a "global early warning system." Although this call has not yet been answered, many recognize that an international clearinghouse serving as a conduit for the gathering and dissemination of cyber security information would greatly increase the ability of administrators to secure their systems against attack.

3.2.2 Information gathering

In the long term, a central clearinghouse could have an equally important impact on information gathering. To collect data effectively on cyber attacks, an information clearinghouse requires the trust of businesses.

⁷⁴Schneier, Bruce. (2001, February). Schneier on Security: The Insurance Takeover. *Information Security Magazine*. http://www.infosecuritymag.com/articles/february01/columns_sos.shtml [2002, April 4].

⁷⁵The Bugtraq mailing list is a popular forum for sharing and discussing newly discovered vulnerabilities. The list archives are available online at: http://online.securityfocus.com/archive/1

⁷⁶See http://cassandra.cerias.purdue.edu/main/index.html

⁷⁷Cassandra requires that you manually search its database and register for each package in which you are interested. Further, it only lists packages for which vulnerabilities have already been found: system administrators cannot register for packages that so far have no identified vulnerabilities. Finally, the project depends on other sources for its information and can thus only be as effective as those sources.

⁷⁸Mukundan, P. (2002). Laying the Foundations for a Cyber-Secure World. In *Transnational Cyber Security Cooperation: Challenges and Solutions* (p. 2). Washington, DC: CSIS Press. Forthcoming.

Businesses have disincentives for sharing information about attacks on their infrastructure. They fear liability, loss of consumer trust, hindrances imposed by law enforcement, and the revelation of sensitive information.

"It should be stressed, though, that the reporting of an incident is not the same as making it public. Setting up a confidential reporting centre to forward information to regulatory authorities and law enforcement, and provide advance warnings to business of threats on the horizon, could help overcome the disinclination of companies to report an attack."

In order to alleviate these concerns, an information clearinghouse could filter the reports that it receives from businesses and other organizations, removing sensitive information before it distributes the reports more broadly.

Even without the concerns of making security breaches public, businesses' fear of a disruptive investigation often makes them reluctant to involve law enforcement. System administrators in industry particularly fear the confiscation of a server or other mission-critical equipment for use as evidence. This fear, likely arising from the unfortunate Steve Jackson Games case of the early 1990s,⁸⁰ is not without merit. Most law enforcement agencies now understand the need to work with businesses to ensure minimal disruption and to obtain useful evidence without confiscating entire machines. In developing States, however, law enforcement personnel may lack the necessary training that enables work at this skill level. This problem is further addressed in Section 3.5 below on "Providing assistance to developing nations".

The Piracy Reporting Center in Kuala Lumpur is a good model for how to respond to private sector concerns about disclosure. Similar disincentives to information sharing, and to engaging the assistance of law enforcement, plagued the maritime shipping industry in the early 1990s as it faced a rising threat from piracy. The International Maritime Bureau (IMB) responded by creating the Piracy Reporting Center. This centre began gathering data concerning attacks and using that data to engage the assistance of the appropriate law enforcement officials. The businesses preferred interacting with the private IMB to working with law enforcement. The IMB was also able to use the collected data to demonstrate the magnitude of the problem and thus to engage policy-makers. Indeed, the "IMB Piracy Reporting Center became a catalyst for most antipiracy initiatives in the region."81

Another problem faced by information sharing initiatives relates to the interaction of public and private agencies. The military and intelligence communities are undoubtedly reluctant to share all of their information with most other States and with private entities: The US National Infrastructure Protection Center (NIPC) specifically addresses this issue: "before disseminating such information, the NIPC coordinates with the intelligence community to protect national security interests." The military and intelligence communities may, however, share such information with States with which they are closely allied. Situations of this nature are often best served by bilateral, frequently informal, efforts. The NIPC is participating in informal bilateral efforts with watch centres in at least five different nations, ⁸³ and the UK, Canada, and Australia each have "liaison representatives" at the NIPC headquarters. The NIPC has also worked with other nations to advise them on the establishment of their own infrastructure protection centres.

The efforts of the NIPC and other bilateral arrangements have been useful. However, a multilateral effort can be more effective simply because it has more sources for the gathering and dissemination of information.

80For more information, see "EFF "Legal Cases - Steve Jackson Games v. Secret Service - Phrack Case - Operation Sundevil" Archive" at: http://www.eff.org/Legal/Cases/SJG/

82National Infrastructure Protection Center (NIPC). *Information Sharing – Outreach*. http://www.nipc.gov/infosharing/infosharing.htm [2002, March 28].

⁷⁹Mukundan, 3.

⁸¹Mukundan, 6.

⁸³ Vatis, 8.

⁸⁴Vatis, 8.

The trust problem that results in a preference for bilateral relationships can be overcome: States can reserve the right to withhold information that they believe to be of a strategically important nature.

Among the many information sharing efforts, the Forum of Incident Response Teams (FIRST) is a good example of an informal multilateral approach. FIRST is composed of public, private, and academic computer security incident response teams from more than twenty different countries. It "aims to foster cooperation and coordination in incident prevention, to prompt rapid reaction to incidents, and to promote information sharing among members and the community at large." FIRST disseminates information largely through mailing lists, conferences and symposia. FIRST also has regional equivalents, such as the Asia Pacific Security Incident Response Coordination (APSIRC). As described in Section 2.1 however, informal efforts do not always scale well. As a result, FIRST, APSIRC, and other similar groups may not be able to serve as a useful resource to the entire international community of system administrators.

CERT/CC is a multilateral initiative that has served as an international information clearinghouse since its inception in 1988. CERT/CC collects and disseminates information from industry, academic, and government sources. It also has projects under way to provide tools that will enable system administrators to better secure their networks and information systems. CERT/CC is a formal effort in that it is funded by the US Government and was charged with specific tasks at its creation. In its interaction with other organizations, however, CERT/CC is informal. No agreement or law requires businesses and other groups to report security incidents to CERT/CC. They do so only in the belief that, in the long term, it serves their best interests.⁸⁷

Although the mission of CERT/CC may be valuable, some have expressed dissatisfaction with the centre's effectiveness. 88, 89, 90 One complaint, that CERT/CC is too slow when announcing vulnerabilities, is an aspect of the responsible disclosure debate mentioned in Section 3.1 above. CERT/CC is said to be more generous than widely accepted industry practice in allowing software makers time to examine vulnerabilities and create patches for those flaws. Critics argue that software makers do not need this extra time. Furthermore, because these vulnerabilities may be already known in the criminal community, attackers may have the opportunity to exploit them before system administrators are aware of their existence. Critics also point to the lack of detail in CERT/CC advisories. While these criticisms may have validity, they also may fail to take into account the constraints with which CERT/CC is faced. CERT/CC tries to achieve the difficult balance of appeasing vendors while simultaneously serving the broader community of system administrators.

Another existing form of clearinghouse is industry-specific: the Information Sharing and Analysis Centers (ISACs) in the United States are examples. The ISACs were created with the NIPC in response to US Presidential Decision Directive 63 and were intended to "serve as the mechanism for gathering, analyzing, appropriately filtering and disseminating private sector information to both industry and the NIPC." While valuable, these organizations have membership restrictions and thus limit the speed and breadth of

⁸⁵Forum of Incident Response and Security Teams. (2002, April 26). FIRST Member Team Information. http://www.first.org/team-info [2002, May 6].

⁸⁶Forum of Incident Response and Security Teams. (2001, October 3). *What is FIRST?* http://www.first.org/about/ [2002, March 29].

⁸⁷CERT/CC. (2002, April 15). CERT/CC Overview, Incident and Vulnerability Trends. http://www.cert.org/present/cert-overview-trends [2002, May 6].

⁸⁸ Martin, Brian a.k.a. Jericho. (2001, April 19). Cashing in on Vaporware. http://www.attrition.org/security/rant/z/jericho.007.html [2002, April 5].

⁸⁹Forno, Richard. (2001, April 21). CERT: The Next Generation. The Demise of the Internet's Last Objective and "Trusted" Organization. http://www.infowarrior.org/articles/2001-03.html [2002, April 5].

⁹⁰Slashdot.org. (2000, October). *CERT and Vulnerability Disclosure*. http://slashdot.org/articles/00/10/08/1815211.shtml [2002, April 4]. See post "CERT is useless nowadays" among others.

⁹¹National Infrastructure Protection Center. (1998, May 22). The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. http://www.nipc.gov/about/pdd63.htm [2002, April 3].

information dissemination – threats to one industry may be applicable to other industries that might not be warned. As a result, the ISACs do not fulfill the general need for a universal agent that collects and disseminates information from all industries and all countries.

Pottengal Mukundan, of the International Chamber of Commerce (ICC), cites his organization as uniquely suited to serve as both an information gathering and dissemination centre and as an intermediary between the public and private sector. As a non-profit, business-oriented association, he believes that the ICC is accepted as a trusted third party for the receipt of sensitive information. The ICC's policy experience and prior efforts may also enable it to effectively advocate policy solutions to many governments.⁹²

We believe that current approaches serve important functions: industry clearinghouses like the ISACs serve as a focus for industry specific concerns and informal efforts like FIRST and APSIRC can help build trusted relationships between incident response teams. Nonetheless, a universal, formal, multilateral effort is worthy of exploration to fulfill the needs of information gathering and dissemination. Vertical industry efforts lack the breadth, and informal efforts lack the reach needed to ensure more secure information systems and network infrastructures. While the CERT/CC model has been criticized, more resources and a strategic focus might enable this organization to be more effective. Otherwise, a new organization created from a coalition of States might prove to be the most effective approach.

3.3 Halting cyber attacks in progress

While information sharing will help to enable proactive efforts at securing networks, system administrators also need reactive measures to assist in ending attacks that have already begun. This need is particularly evident in denial of service attacks, which can be of extended duration and which can cripple a business while they occur.

3.3.1 Automated tracing

Halting attacks in progress and investigating attacks are both hampered by the inability to easily identify and locate attackers. Because packet source addresses are easily forged, the only way to identify an attacker with confidence is to trace the path taken by the packet through the routing infrastructure of the Internet. This tracing is a manual process and essentially requires the cooperation of every network operator between the attacker and their target. The inability to trace automatically the source of an attack in real-time significantly impairs the ability of targets and law enforcement agencies to respond to incidents.

Automating the identification of attackers can be achieved by making changes to the structure of the Internet: for example, altering the routing system or the protocols⁹³ used in packet switching.

"There is a tension between the capabilities and vulnerabilities of routing protocols. The sharing of routing information facilitates route optimization, but such cooperation also increases the risk that malicious or malfunctioning routers can compromise routing. In any event, current Internet routing algorithms are inadequate because they do not scale well, they require central processing unit (CPU)-intensive calculations, and they cannot implement diverse or flexible policies. Furthermore, no effective means exist to secure routing protocols, especially on backbone routers. Research in these areas is urgently needed." 94

Changes to the protocols of the Internet have proven difficult, however, as evidenced by the slow adoption of IPv6. 95 Adding functions to the routers and switches that compose the core of the Internet may be a more

.

⁹²Mukundan, 8-9.

⁹³One proposal would require the use of a single additional bit per packet. See: Luciano, Elizabeth. (2002, April 4). *UMass computer scientist offers a new way to track Internet vandals*. http://www.eurekalert.org/pub_releases/2002-04/uoma-ucs040402.php [2002, April 18].

⁹⁴Schneider, Fred B. (Ed.). (1999). *Trust in Cyberspace* (p. 243). Washington, DC: National Academy Press.

⁹⁵Systems on the Internet use the Internet Protocol (IP) to communicate. Version six of that protocol is designed to supercede version four, the current standard.

viable possibility: relatively inexpensive solutions to the problem of tracing packets exist and require only limited hardware and software additions to current routers. Ghanges of this nature could be phased in gradually by incorporating them into newer products and allowing the upgrade cycle to disseminate the new devices.

The nature of the current standards process suggests that any change to the structure of the Internet, or to the devices that compose the core of the critical network infrastructure, have to be made through an established multilateral effort. The IETF could create new standards focused on security in order to effect the necessary changes. The IETF standards process, however, can be slow and the implementation of new standards is never certain.

Another approach takes into account the fact that Internet service providers (ISPs) and network backbone operators are the most significant players in the tracing of packets. Should those groups agree to make the necessary changes to support automated tracing, they could have a considerable impact. Even partial adoption could significantly ease the challenge of locating attackers by decreasing the number of network operators who must manually search their logs for evidence. ITU could play a central role in determining the most appropriate solution to this problem and in coordinating its acceptance with network operators and telecommunications carriers.

Automating the identification of attackers, however, has significant consequences for the culture of the Internet and might curtail some of the benefits that are currently taken for granted. For example, the ability to easily identify attackers will also increase the ease with which *any* Internet user can be traced and identified. The opportunity for users to remain anonymous in their communication will be severely curtailed. Moreover, the level of anonymity currently available enables free speech for those who might otherwise be persecuted for their beliefs—is the benefit of greater security worth the cost of decreasing anonymity? Such changes should not be taken lightly.

Automated tracing is not an easy goal; indeed, it may not be a feasible or an entirely beneficial one. Nonetheless, it would greatly improve the active defence measures available to system administrators and assist in the investigation of attacks. An international effort to consider this goal may be valuable.

3.3.2 Cooperation and coordination with infrastructure operators

Stopping an attack in near real-time is an important means of limiting damage to the target and is therefore a critical objective for the target entity. Because of the limitations faced by law enforcement agencies and the speed with which these agencies are able to respond, the target itself may be more effective at quickly stopping the attack. "The propagation rate of potential destruction demands instantaneous response and is, therefore, troublesome to a legal system that is slow and deliberative." Even the type of structure proposed by the COE Cybercrime Convention might not be able respond to attacks rapidly enough.

In order to stop attacks, the target would likely need to obtain the cooperation of infrastructure operators. Such cooperation is complicated by the transnational nature of the Internet. A further challenge is that the involved parties, targets and infrastructure operators, are often private entities that do not always have the resources or incentive to respond. Organizations, particularly private entities, may need a mechanism for efficiently coordinating with each other and with infrastructure operators to halt or minimize the damage from an attack in progress.

A British ISP, Cloud 9, recently suffered a distributed denial of service attack that forced it to declare bankruptcy. 98 Had Cloud 9 been able to quickly locate and contact the ISPs serving the attacking computers,

⁹⁶Snoeren, Alex C. et al. (2001, August). Hash-Based IP Traceback. *Proceedings of the ACM SIGCOMM 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*. http://nms.lcs.mit.edu/~snoeren/papers/spie-sigcomm.pdf [2002, May 6].

⁹⁷Branscomb, Anne Wells. (1993). Jurisdictional Quandaries for Global Networks. In L. M. Harasim (Ed.), Global Networks: Computers and International Communication (p. 83). Cambridge, MA and London: The MIT Press.

⁹⁸Wearden, Graeme. (2002, January 23). DoS attack shuts down ISP Cloud Nine. ZDNet (UK). http://zdnet.com.com/2100-1105-820708.html [2002, April 5].

it might have been able to limit the damage caused by the attack and retain its solvency. A transnational structure for soliciting, and perhaps requiring, the aid of infrastructure operators could contribute greatly to the ability of entities to limit the damages caused by attacks.

Most current approaches for solving this problem are informal bilateral efforts. System and network administrators at ISPs form personal relationships with their counterparts at similar organizations. This environment is effective when a relationship exists; understanding each other's needs, administrators move quickly to respond to attacks. Problems arise when administrators do not have relationships with the necessary ISPs or when organizations that are not themselves ISPs need assistance. The transnational nature and scope of the world's interconnected networks suggests that far too many ISPs exist for a network of informal bilateral relationships to suffice: bilateral efforts do not result in a sufficient breadth of coverage. Those relationships that do exist are also most likely between ISPs—other types of business are less capable of obtaining the needed cooperation.

The drawbacks of bilateral efforts suggest that a near-universal multilateral effort might be more effective. FIRST is one significant informal multilateral effort in this area, but its membership may not yet be large enough to ensure adequate breadth of coverage; not all infrastructure operators are members of FIRST.

While a multilateral effort appears to be a more appropriate solution than bilateral efforts, choosing between a formal and an informal effort is less clear. Informal efforts may be unreliable in providing assistance between organizations. However, a growing awareness of the nature and extent of the problems of cyber crime may cause ISPs and other infrastructure operators to be more universally receptive to requests for assistance. A formal agreement, on the other hand, offers the benefit of contractual obligations and could give organizations a means of resolving disputes that arise from the aid process. Such an agreement would also give businesses the certainty and trust that promotes the development of e-commerce.

While we know of no formal, multilateral effort toward the goal of halting attacks, we believe this is a useful area of potential cooperation. ITU may be well situated to enable this type of effort. Because network operators are particularly important in halting cyber attacks, ITU could play an important role in forging agreements for coordination between operators and particularly with telecommunication carriers.

3.4 Coordinating legal systems

The trans-border nature of the critical network infrastructure inhibits effective prosecution of cyber criminals; without legal system coordination, jurisdictional issues may protect attackers from prosecution. In the current legal environment, most adversaries can attack without risk – they fear no reprisal and will not stop until they achieve their objective or lose interest. The ability to effectively prosecute cyber criminals and terrorists is one means of imposing risk on the actions of an attacker.

Prosecution of attackers, however, is made extremely difficult by the interjurisdictional nature of cyber space. Imposing criminal liability often necessitates cooperation and coordination between States in their efforts to prosecute attackers. This scenario introduces important questions for law enforcement, which may be divided into two categories: problems of legal harmonization and problems of investigation procedures. These issues are addressed in the sections that follow.

3.4.1 Harmonization of laws

The problem of multiple jurisdictions having interest in a single crime is not unique to information networks, although these networks have exacerbated the challenge. States have a number of pre-existing tools for dealing with such situations, including formal bilateral agreements such as MLATs or informal bilateral tools like letters rogatory. However, treaties and conventions are useful in engaging the cooperation of States only if the actions of the attacker are considered a crime in each of the involved countries, a requirement known as dual criminality.

Unfortunately, the explosive growth of international networks has outstripped the pace of lawmaking with regard to crime that is strictly cyber by nature. A recent survey sheds light on the international existence of

⁹⁹ Letters rogatory are described in footnote 19.

laws regarding cyber crime.¹⁰⁰ The fact that only 37 of 185 contacted States responded to the survey might itself indicate a lack of recognition regarding the importance of this realm. Over 60 per cent of those States that did respond criminalized the unauthorized destruction of, alteration of, or rendering inaccessible of data. 51 per cent penalized the unauthorized acquisition of data, although for 32 per cent of the respondents this action was only criminal if preceded by unauthorized access to the system. For 29 per cent, the law distinguished between the types of data that is acquired without authorization. Although the survey indicated some progress, it also highlighted the lack of widespread harmonization of laws in respect of cyber crime.¹⁰¹

The Love Bug virus of 2000¹⁰² is a good example of the necessity of dual criminality for the imposition of criminal liability on cyber crime. This virus was quickly traced to the efforts of Onel de Guzman, a student in the Philippines. However, at the time his actions were not a crime in the Philippines, and so he could not be prosecuted or extradited. The effective prosecution of cyber attackers, therefore, requires some level of harmonization of laws between different States.

The current successes achieved through the use of MLATs (formal, bilateral treaties) and other existing treaties demonstrate the possible use of bilateral efforts in this arena. Letters rogatory serve as an informal bilateral means of cooperation where formal efforts have not been established. Despite these successes, the global penetration of the Internet and the example of the Love Bug virus indicate that attacks may originate from any State. To ensure adequate coverage, therefore, a coordinated multilateral effort may be a more useful approach.

The most prominent multilateral effort in this area is the Council of Europe Convention on Cybercrime. Although harmonization of laws is just one target of this treaty, much of the rest of the work lies upon this foundation. The Stanford Draft Convention also attempts to achieve a harmonization of laws, but with a different emphasis. Universal participation in this treaty or any other effort that results in the harmonization of laws will help to eliminate "safe havens" for attackers and increase the risk at which they place themselves through their actions.

Formal agreements seem more likely to encourage the universal participation that will be most effective in enabling the prosecution of cyber attackers. Indeed, formal agreements appear more suitable for a variety of reasons:

"Our experience in the United States, at least, suggests that it is easier to pass enabling legislation if it is required by an international agreement and, conversely, that the formality of negotiations for international agreements allows for public input at an early stage, ensuring that whatever agreement is reached is politically palatable." ¹⁰³

A less formal effort, such as in the OECD Guidelines where States are encouraged to enact legislation voluntarily, making acts of cyber crime illegal, could be a useful interim measure. One potential difficulty in formal or informal efforts is that developing nations may lack the resources necessary to create this legislation. Efforts such as the ongoing American Bar Association's Cyber Crime Project, however, can provide those nations with a framework legislation that they may customize to suit their specific needs. We address this problem again in Section 3.5.

¹⁰⁰Kaspersen, H.W.K. and Lodder, A.R. (2000, April 15). Overview of the Criminal Legislation Addressing the Phenomenon of Computer-Related Crime in the United Nations Member States. United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (UNAFEI) Report. http://www.rechten.vu.nl/~lodder/papers/unafei.html [2002, April 10].

¹⁰¹Goodman, Marc D. and Brenner, Susan W. (Draft 2002, March). The Emerging Consensus on Criminal Conduct in Cyberspace. Not yet published.

¹⁰²For information on the estimated worldwide damages caused by this virus and others, see: http://www.computereconomics.com/cei/press/pr92101.html

¹⁰³Litt and Lederman, 8.

¹⁰⁴American Bar Association. *International Cyber Crime Project of the ABA Privacy and Computer Crime Committee*. http://www.abanet.org/scitech/computercrime/cybercrimeproject.html [2002, April 5].

3.4.2 Investigation procedures

While harmonized laws enable the extradition of alleged cyber criminals, successful prosecution also requires the ability to manage investigations that cross national boundaries. These investigations are fraught with difficulties, especially in coordinating the efforts of law enforcement in different jurisdictions. Transnational investigations are common and their difficulties are well known. However, the architecture of information networks creates challenges that are unique or unusually troublesome with respect to investigations of cyber crime.

One of the challenges is in tracing an attack, as described in Section 3.3.1. Investigators must frequently work with both law enforcement and private entities in a potentially large number of different States merely to gain some measure of information about the source of an attack and the identity of the attacker.

Investigators face another constraint with regard to this tracking: its urgency. The logs and other sources of information that help investigators locate and identify attackers are often temporary in nature. Infrastructure operators constantly generate huge volumes of this information; most do not have the resources to retain all of it for more than a short time. The slow pace of a normal investigation will not suffice in this instance – the infrastructure operators who hold the evidence must move quickly to secure it. Another reason for urgency is the danger that a skilled attacker might return and erase any remaining evidence. ¹⁰⁵ A cyber investigation thus often requires the rapid cooperation of multiple governments and private entities located within foreign States.

Without investigation, determining whether a cyber attack is prompted by criminal, ideological, or strategic purposes is extremely difficult to determine. In other words, initially cyber terrorism, cyber espionage, information warfare (State sponsored acts), and cyber crime appear the same to a victim.

If an attack is State sponsored, the attacking State may find that the victim State requests its aid in prosecuting the attacker. The attacking State may therefore have strategic reasons for denying aid to law enforcement officials in the victim State. "Although international agreements may contain exceptions that permit a State to decline to cooperate based on its 'national interest,' a State would presumably prefer not to invoke such an exception, in effect admitting its own activities." ¹⁰⁶ States could avoid this situation by only using bilateral agreements and by limiting those agreements to other States that they deem to be allies (and therefore, presumably, States against whom they will not practice information warfare or cyber espionage¹⁰⁷). Some nations may be more comfortable acting in bilateral agreements and thus may be reluctant to ioin a multilateral treaty.

The FBI's Legal Attaché (LEGAT)¹⁰⁸ offices are a good example of how increasing informal bilateral cooperation can support investigation. "The LEGATs allow the FBI to develop on-the-ground relationships with host-country investigators and to provide a liaison to expedite assistance between the United States and host country, in both directions."¹⁰⁹ Another example of informal relationships are those developed through the various training programmes offered by the NIPC. The NIPC works to train law enforcement agencies in different countries on the unique challenges of cyber investigations. A significant benefit of these informal efforts is the ability to request and receive assistance rapidly, without the impediments of formal channels.

Formal bilateral agreements are generally easier to negotiate and can be more specific than multilateral efforts. MLATs are the most common example of formal bilateral agreements used to counter cyber crime. They provide means for requesting assistance and information in the course of an investigation.

¹⁰⁵Vatis, 3.

¹⁰⁶Litt and Lederman, 9.

¹⁰⁷The oft-denied Echelon espionage program run by the United States, Great Britain, Australia, Canada and New Zealand runs contrary to this theory, however. For more information, see: ZDNet UK, News Special: Echelon, http://www.zdnet.co.uk/news/specials/2000/06/echelon [2002, May 2].

¹⁰⁸Federal Bureau of Investigation. About Us – Legats. http://www.fbi.gov/contact/legat/legat.htm [2002, April 5].

¹⁰⁹Vatis, 8. Much of the other information in this paragraph was also taken from this source.

Unfortunately, they do not provide investigators with an assuredly timely means of preserving transient evidence. MLATs have two additional shortcomings: they may not exist between each of the necessary countries involved in an investigation¹¹⁰ and they may not address computer crimes.¹¹¹ These formal efforts are valuable, however, because they offer the participating States some degree of assurance that they will receive the aid that they request. If States do not have MLATs, they may have to rely on letters rogatory. This instrument is completely unsatisfactory for the required pace of a cyber crime investigation. Even the most expedited and urgent requests conveyed through a letter rogatory may require more than a month to fulfill.¹¹²

Despite the ease of negotiation, greater specificity, and tailorability of bilateral agreements and efforts, however, they seem likely to be insufficient for effectively addressing cyber crime. Bilateral efforts do not scale for situations where multiple governments are involved. Moreover, the number of bilateral agreements necessary to achieve universal participation is completely impractical, yet this level of participation is necessary to deny cyber criminals any safe havens. It would seem, then, that a multilateral treaty would provide the most utility in this situation. Such a treaty would ideally enable nations to request and receive timely assistance from any other State and from multiple States if necessary.

As in bilateral agreements, informal multilateral efforts are generally easier to create than more formal agreements. When the volume of incidents or the number of participants is small, informal multilateral efforts can also be more expeditious in operation than formal. One such effort is the G-8 Subgroup on High Tech Crime. This group has focused its work in four different areas.

The first area was the establishment of 24x7 (twenty-four hours a day, seven days a week) watch centres in all of the G-8 States and several other States. These watch centres provide a central point of contact for law enforcement agencies of the participating nations. This informal network has increased the speed and efficiency of communications between participating countries and has thus improved the process of preserving evidence in cases of cyber crime. A second achievement was a training symposium held for law enforcement personnel of the G-8 States. Third, the group reviewed the legal systems of their States and worked to ensure complete coverage of cyber crime and harmonization among the different States. Finally, the G-8 Subgroup collaborates with industry in an effort to "improve law enforcement's ability to locate and identify cyber criminals, including [taking] steps to address issues such as data preservation and retention, real-time tracing of communications, ISP cooperation with law enforcement, and user authentication." 113

The G-8 effort has had some success: it has fostered informal cooperation between law enforcement agencies from different States, helped identify important issues for international cooperation in regards to network security, and served as a model for subsequent multilateral efforts.¹¹⁴ Nonetheless, the Subgroup's limited coverage and lack of uniform process reveal the need for a more formal multilateral effort such as the COE Convention or the Stanford Draft Treaty.

3.5 Providing assistance to developing nations

Developing nations face severe scarcity of resources that both decrease their own security posture and prevent them from effectively providing assistance in international efforts. The global nature of the Internet requires more than just a need for States to have harmonious laws. The enforcement of those laws requires cooperation among trained personnel in the involved States and thus States must have the capability to fulfill the requests of foreign law enforcement agencies. This is difficult for developing nations; even the most

¹¹⁰The United States currently has nineteen MLATs in force and fifteen more that are signed but not yet in force. From: U.S. Department of State. *Mutual Legal Assistance in Criminal Matters Treaties (MLATs) and Other Agreements*.

¹¹¹ Vatis, 3

¹¹²United States Department of Justice, Title 9, Criminal Resource Manuel, 275 Letters Rogatory.

¹¹³Vatis, 5. Much of the other information in this paragraph was taken also from this source or from: National Cyber crime Training Partnership. (2000, March). *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet*. http://www.nctp.org/append10.html [2002, April 5].

¹¹⁴ Vatis, 5-6.

networked countries are struggling to find the resources and knowledgeable personnel to counter cyber crime. Industrialized countries must, therefore, aid developing countries where resources are insufficient to assist in the investigation and prosecution of cyber criminals.

One example of this assistance is the informal bilateral efforts of the NIPC. The NIPC has offered cyber investigation and forensics training programmes to many international law enforcement agencies.

"This training serves not only to make foreign partners more capable of assisting in international investigations and of addressing cyber crime within their own countries, but also to establish personal relationships and trust among international investigators, which prove invaluable when an incident occurs and assistance is required." 115

The training offered by NIPC is run through classes held in the United States, at the International Law Enforcement Academies located in Hungary and Thailand, and in symposia co-sponsored with other nations. Since the founding of NIPC in 1998, Japan, the UK, Canada, Germany, and Sweden have moved to create agencies with similar function in their respective countries. However, bilateral efforts are likely to be insufficient for the goal of providing assistance to developing nations; many States will need this assistance, and those States able to contribute would undoubtedly prefer not to bear the burden alone.

A formal, multilateral effort may be a good approach to providing adequate levels of assistance in order to reduce cyber crime. Models for such efforts are already in existence. In particular, the International Civil Aviation Organization (ICAO) uses contributions from industrialized States to invest in training and other resource enhancement for developing States. A similar model might work for information security, particularly with respect to network infrastructures. As mentioned in Section 2.3, the Stanford Draft Convention would create the AIIP to coordinate efforts to reduce cyber crime and to provide assistance to developing countries so that they can fulfill their obligations under the treaty.

The disparity in capabilities between countries reduces opportunities to pursue prosecution in cyber crime cases. Countries with more resources may address this disparity by providing aid to developing nations. As in international aviation, the provision of aid is likely to require a formal multilateral agreement; the disbursement of this aid may further require an international organization such as that proposed in the Stanford Draft Convention.

4 Unintended consequences, national strategies, and topical concerns

"For every complex problem, there is a solution that is simple, clear, and wrong."

- H. L. Mencken¹¹⁶

Among the opportunities for international cooperation, Section 3 targets five specific areas. Each of these areas is at best a partial solution that leaves many security questions unresolved. This section reviews issues that governments and organizations such as ITU address when they negotiate or implement new international measures for critical infrastructure protection. This material is intended to raise questions, not to provide answers. Indeed it is neither possible nor desirable to give simple or exact answers. The problem is not necessarily that these questions cannot be answered, but that answering them wisely requires careful planning at both national and international levels.

These issues are divided into three groups based on the types of difficulties they present. The first group consists of system effects related to the complexity of defending networks from hackers who learn and who change their strategies. The second group involves the difficulty of separating security issues from other policy concerns. The third group contains strategic planning issues that cannot be separated from the exigencies of other national concerns. Resolving issues in the third group requires each nation to develop its

¹¹⁵ Vatis, 8. Much of the other information in this paragraph was also taken from this source.

¹¹⁶Cited in Burnett, Sterling. *Opinion Editorial: Gun Lawsuits Hurt All Of Us.* National Center for Policy Analysis. http://www.ncpa.org/oped/sterling/dec1299.html [2002, May 1]

own strategy balancing its security needs with its financial and technical constraints. Finally, we address two areas to which all these concerns are relevant: cyber-terrorism and active defence.

4.1 Unintended consequences of system effects

Unintended consequences have been a problem in foreign policy decisions for millennia, and in foreign policy research for many years. Robert Jervis, along with other recent researchers, has attributed some unintended consequences to "system effects," those effects that arise when "a set of units or elements is interconnected so that changes in some elements or their relations affect changes in other parts of the system." System effects are different from other varieties of unintended consequences in that they can occur even in very simple systems where overlaps with other policy areas can be ignored. While they can occur in physical and biological systems as well, system effects in politics are often found in situations where the people affected by a policy alter their behavior in response to a policy change. One difficulty they pose for policy-makers is that in certain cases, the complexity of the interactions can cause simple policies to have an effect opposite to their goal. Jervis mentions double-hulled oil tankers as an example – if building safer, more expensive oil tankers causes companies to decrease spending on other security measures or cause tanker captains to take more risks, it might lead to more oil spills, rather than less. 118

4.1.1 System effects applied to security

In the security domain, the people affected by policy changes include attackers, defenders, international allies, system administrators, and ordinary users. Any of these groups could cause a reverse result by modifying their behavior when security policies change. Some challenge-seeking hackers, for example, are more likely to attack servers renowned for their strong security measures. Users may respond to requirements for longer passwords and biometric identification by writing their passwords on their desks and by leaving the doors to restricted areas ajar. The free rider problem discussed in Section 3 is an international example of a potential reverse result – an initially successful multilateral approach may tempt some States to neglect their own responsibilities, possibly undermining the approach's subsequent success.

Designing policies that avoid such system effects is never easy, but the more effectively defenders anticipate the responses of attackers, users, and allies to new security measures, the more likely defenders are to achieve their goals. Better policy design and awareness of system effects have been suggested as good ways to reduce the odds of complexity-related policy failures. Improving the ability of defenders in other countries to anticipate reverse results may be an important task for the information sharing and international assistance mechanisms discussed in Section 3.

4.1.2 Iterative attack/defence cycle

Two important system effects in cyber defence are the danger of attempting absolute guarantees and the ability of hackers to find new vulnerabilities. The danger of guarantees is that many "guaranteed" systems do not live up to their name. If the guarantee leads to the neglect of other security measures, or to routing a greater proportion of critical network infrastructure through a guaranteed system, it can lead to greater damage if hackers later discover a security hole that proves the "guarantee" wrong. Both national and international security policies, therefore, should be careful to avoid too readily declaring a network to be "secure."

In a related problem, the ability of hackers to discover new vulnerabilities ensures that it is never enough for defenders to close all known security holes. Instead, defenders must also learn, and they must use flexible strategies capable of responding to new and unexpected attacks. If defenders do not have the resources to continuously update and improve their security, they may be better off concentrating on recovery measures instead of on prevention.¹¹⁹

¹¹⁷ Jervis, Robert. (1997). System Effects: Complexity in Political and Social Life (p. 6). Princeton, NJ: Princeton University Press.

¹¹⁸Jervis, 7-8.

¹¹⁹Lukasik et al, 36-37.

Lukasik et al. describe this learning process as an iterative cycle of repeated attacks and defences:

"Absolute defence against attack has rarely been achieved. Each defensive measure generates a countermeasure by an attacker, driving the defender to adopt ever stronger measures. This sequence of action and counteraction is common in adversarial relationships, and it is most obvious and best understood in the interaction of opposing military forces." ¹²⁰

Solutions to the challenges posed in Section 3 may be more effective in responding to changing cyber threats if they are implemented with the iterative attack/defence cycle in mind. For example, information sharing is essential to mounting global responses to new threats. Other methods such as harmonizing laws will be most effective if they include mechanisms for updating laws to address new cyber crimes that exploit legal as well as technological loopholes. This need is similar to the need to update anti-narcotics regulations to prohibit new synthetic drugs that mimic the effects of banned substances.

4.2 Unintended consequences of policy overlap

The second group of difficulties we consider are the unintended consequences that can occur when two or more policy areas overlap. Such overlaps can lead to important values being mishandled by non-experts, to the 'capture' of regulatory bodies by the industries they regulate, or to increased opposition to negotiating new agreements. Overlap-related consequences are sometimes easier to address than system effects since they do not involve reverse results – a policy-maker with a reverse result may have no good alternative but to undo the policy, while a policy-maker with a combination of one good and one undesired result may be able to institute additional policies to compensate.

A classic case of unforeseen consequences leading to political difficulties is the arbitration system created by the 1994 North American Free Trade Agreement (NAFTA). The arbitration panels were established along a World Bank model initially designed to provide government compensation to the foreign owners of seized property. Lawyers in all three NAFTA countries (the US, Canada, and Mexico) are now expanding the anti-expropriation clause in ways that have led some States to warn that "a new set of foreign investor rights" has compromised their ability to govern. One case resulted in the arbitration panel's reinterpretation of the Mexican Constitution. In the US, meanwhile, Eric Biehl, a former Commerce Department official "wonders, how does some mechanism on a trade agreement that no one thought much about suddenly get used to open up a whole new appellate process [effectively getting] around the US judicial system." These cases are complicating efforts to negotiate free-trade agreements with Chile and the 34-nation Free Trade Area of the Americas.

The Telecommunications Reform Act in the US presents another good example of the unintended consequences of policy efforts. As a result of the act, many switches and other pieces of critical network equipment have been collocated and are now much more vulnerable to a single physical attack or catastrophe. 122

4.2.1 Intellectual property

Intellectual property is an area that might face unintended consequences under cyber crime regimes. Cyber crimes frequently involve intellectual property issues – many intrusions involve either the theft of trade secrets or attempts to use servers to distribute illegally copied files known as "warez." At the same time, there are wide differences in how different nations define intellectual property rights and in how they balance the concerns of copyright owners with the concerns of content users and the need to protect free speech. These issues are so complex that negotiations involving them could cause long delays in negotiating cooperation against cyber crimes that directly threaten critical infrastructures.

¹²⁰Lukasik et al, 12.

¹²¹Magnusson, Paul. (2002, April 1). The Highest Court You've Never Heard Of (p. 76). Business Week.

¹²²Lukasik, Stephen. (2001, October). *Responding to Cyber Threats: The International Dimension* (p. 17). Georgia Tech Information Security Center & Stanford University's Consortium for Research on Information Security and Policy.

It may be best, therefore, that international agreements on cyber crime sidestep these issues by focusing on crimes that threaten the infrastructure itself. Intellectual property issues are better addressed in other forums where more intellectual property expertise is available and where potential consequences can be examined more carefully.

4.2.2 Civil rights

A second important area of potential overlap is the effect of global criminal treaties on individual States' civil and human rights laws. Different beliefs about human rights often inhibit international cooperation in criminal investigations and in extraditing suspects. In a recent case, for example, Brazil refused to extradite Mexican pop star Gloria Trevi to face charges in Mexico after Trevi gave birth on Brazilian soil. Different legal standards regarding the death penalty and the rights of minors have also created friction between US investigators and their European counterparts. While the death penalty is not currently used in cyber crime cases, some nations may raise concerns about how cyber crime treaties handle the rights of the accused. To which countries would the United States, Brazil, or Sweden be willing to extradite a teenager hacker accused of cyber crime?

A reduction of the level of anonymity available on the Internet, mentioned as a potential side effect of automated tracing and discussed in Section 3.3.1, could have a significant effect on the civil rights of users. While decreasing anonymity may reduce the amount of cyber crime on the Internet, it may also reduce free speech. As has been mentioned, the current level of anonymity affords some protection to those who hold socially or politically unpopular views.

4.3 National strategies and national needs

The final category of inherently difficult questions includes those issues that require carefully considering the circumstances of individual nations. One should note that although these issues address national needs, they are not necessarily national-level issues, but may influence both the participation in and the negotiation of bilateral and multilateral agreements.

Even the strongest international regimes are most effective when they are supported by comprehensive national strategies. As noted in Section 2, one of the advantages of informal and bilateral agreements is that they can be quicker to negotiate and to change than formal and multilateral agreements in response to the evolving threats of the attack/defence cycle. National strategies, requiring no outside negotiation, may be quicker at applying the goals of international regimes to new circumstances than either bilateral or multilateral agreements. The European Union's human rights laws, for example, can make progress either via EU-wide decisions, or by groundbreaking court cases in member States.

We present a few elements of national strategies in the following sections. For a detailed discussion, Lukasik et al. present a more comprehensive framework that individual nations can use to develop strategies for infrastructure defence. They review many of the strategic defence options that nations should consider and address the differences in national capabilities.

4.3.1 Cost planning

The iterative, evolving threats described in Section 4.1.2 ensure that no nation can provide maximum defences against every possible threat. Every nation, therefore, must make choices about which local systems to defend and how to allocate their financial and technical resources among different systems and different forms of defence. This process starts with each nation identifying its critical network infrastructures, determining the likely costs of damage to each of those networks, and determining which resources it has available locally and which it may obtain via international assistance.

Lukasik et al. suggest that cyber defenders adopt a standard tool of military strategists, the cost-exchange ratio:

¹²³Lukasik et al, 10-33.

"Put simply, defenders should not expend large amounts of resources on measures that can be cheaply and easily defeated by an attacker. The converse is that defensive measures should be designed to require the offence to spend inordinately greater resources to defeat them."124

An important consequence of this principle is the implication that governments should be willing to accept some losses, especially minor losses that are difficult to eliminate. This choice could be compared to the decisions that prosecutors routinely make to invest less effort in prosecuting small-time crooks. Lukasik et al. go so far as to say that nations with little confidence in their ability to limit or prevent attacks should concentrate their efforts on recovery and on encouraging "greater local self-sufficiency." 125

Choosing which losses to accept requires caution on the part of governments. Lukasik et al. warn that a major cyber attack could occur as either a single massive attack or a series of smaller, distributed attacks. If a minor attack is part of a major pattern, its costs should be measured accordingly. 126

The private sector and software developers

Another issue that often requires attention to national differences is the role of the private sector in the security of critical network infrastructure – and the regulatory options available to governments to influence private owners' security choices:

"[Private and public] owners are likely to have different views of investing in protection. Private owners, faced with loss of revenue and loss of confidence by customers, regulators, investors, and insurers will seek to restore revenues and confidence in their stewardship. Governments will pursue policies that focus on longer term aspects of protection, seeking to reduce cumulative losses, protecting markets, and maintaining law and order." ¹²⁷

Some private sector firms, including the largest telecom companies and major software vendors such as Microsoft, play a significant role in shaping networks around the world. Software liability is one proposed method for bringing large vendors in line with national infrastructure protection priorities. On January 8, 2002, the US National Academy of Sciences suggested that lawmakers consider legislation that would end software companies' protection from product liability lawsuits. Microsoft and other developers have insulated themselves by disclaiming all product liability. "If Firestone produces tires with systemic vulnerabilities, they are liable," says Bruce Schneier, chief technology officer of Counterpane Internet Security Inc., a provider of network protection services. "If Microsoft produces software with systemic vulnerabilities, they're not liable."128

Due to the complexity of different States' regulatory, liability, and antitrust laws, these issues can rarely be addressed without considering national differences closely and without working through national-level court systems. The harmonization of laws discussed in Section 3 may be more difficult to achieve for such complex portions of corporate law than for laws criminalizing cyber attacks.

Liability is not the only means of promoting secure priorities to software vendors. It is also possible that some national governments will find that exercising their market power as buyers of large quantities of software may have a greater influence on market standards than passing legislation.

¹²⁵Lukasik et al, 37.

¹²⁴Lukasik et al, 1.

¹²⁶Lukasik et al. 10.

¹²⁷Lukasik et al, 13.

¹²⁸Bruce Schneier, quoted in Sager, Ira and Greene, Jay. (2002, March 18). Commentary: The Best Way to Make Software Secure: Liability. Business Week Online. http://www.businessweek.com/magazine/content/02 11/b3774071.htm [May 9, 2002].

4.4 **Topical concerns**

4.4.1 **Cyber-terrorism or cyber protest**

One area of concern—cyber-terrorism—involves all three of the difficult factors discussed above. Since September 11, many authors have expressed concern that "cyber-terrorists" might use computer networks to cause damage or violence commensurate with the damage caused by physical terrorist attacks. Plausible scenarios range from terrorists gaining control of remote networks used for dam and water treatment plant operation to interfering with air and sea navigation networks. 129

In practice, however, most political cyber crimes have consisted of vastly less dangerous attacks such as web page defacements. There have been at least three major waves of politically motivated "cyber protest": between the US and China after two military aircraft collided in May 2001; between Israeli and Palestinian hackers through the duration of the Intifada; and between Indian and Pakistani hackers during crises over Kashimir since 1999.

In each of these three incidents, the relevant "national exigencies" included either nuclear weapons, ongoing violent conflicts, or both. Defining cyber-terrorism broadly or rushing to treat cyber protests as an international issue would risk adding unintended consequences to an already dangerous situation. Jervis' analysis of system effects, for example, largely focuses on the risk of feedback loops promoting escalation and/or arms races between nuclear powers.

An appropriate goal for anti-cybercrime efforts in situations like these three is to emphasize reducing tensions and avoiding dangerous feedback loops. Determining how to do so may be difficult; one could argue either that ignoring cyber protests creates the least risk of escalation, or that following negotiated multilateral procedures for handling online protests could give each nation a safety value for its cyber frustrations.

4.4.2 Active defences

Another factor that Jervis and other foreign policy researchers have addressed is the role of offensive/defensive balance in system effects. 130, 131 They suggest that escalation and other dangerous unintended consequences are a greater risk when conditions favour attack strategies over defence strategies; making the attackers bear greater risks gives them reason for restraint.

Applied to cyber security, therefore, Jervis' analysis suggests that active defences might help to reduce system effects and to dampen the cyber protests described in Section 4.4. Active defences are those measures available to the defender that create risk for the attacker. Prosecution is one such active defence, and coordinating international efforts in this regard is discussed in Section 3.4. Other types of active defences are more problematic. They can include anything from identifying the attacker to cyber counter-attacking. Such actions can be appealing to the victim of a cyber attack, particularly if that victim feels that law enforcement is unwilling or inadequately prepared to prosecute the attacker. Their potential to reduce certain system effects, however, must be carefully weighed against other political risks.

The victims and intermediaries of a cyber attack will in many cases be private sector entities. While technologically able to attempt active defences, these entities do not have a legal basis for doing so. In addition, given the difficulties in tracing an attacker, some percentage of active defence measures may be inflicted on innocent parties. By inflicting collateral damage or damage on innocent parties, the defender is

¹²⁹Brenner, Paul and Meese, Edwin (Chairs). (2002). Defending the American Homeland. Washington, DC: The Heritage Foundation. http://www.heritage.org/bookstore/2002/defense/HomelandDefenseweb.pdf [2002, April 30].

¹³⁰Jervis, Robert. (1978, January). Cooperation under the Security Dilemma (p. 167-214). World Politics, Volume 30, Number 2.

¹³¹Powell, Robert. (1991, December). Absolute and Relative Gains in International Relations Theory (p. 1303-1320). American Political Science Review, Volume 85.

likely to become a more easily identifiable target of legal action, negative publicity, and civil liability. "Furthermore, few governments anywhere officially condone vigilantism." ¹³²

Active defences may more logically, then, be considered the province of governments. Governments have a firmer legal basis for such actions¹³³ and do not need to fear liability as private entities do. When responding to an attack that crosses national boundaries, however, a defender may have to interact with devices that are physically located in a different State. Governments are likely to strongly object to any such action, considering it an intrusion of their sovereign domain. "Under these circumstances, particularly if the volume of serious cyber attacks is high, sooner or later visible misidentifications and collateral damage will result and would likely generate international friction between governments."¹³⁴

5. Conclusions

Network infrastructures have become critical to both the daily lives of individuals and the economies of States. Yet, those critical network infrastructures are increasingly vulnerable to attack.

"We have spent years making systems interoperable, easy to access, and easy to use. Yet we still rely on the same methods of security that we did when data systems consisted of large mainframe computers, housed in closed rooms with limited physical access. By doing so, we are building an information infrastructure—the most complex the world has ever known—on an insecure foundation. We have ignored the need to build trust into our systems. However, simply hoping that someday we can add the needed security before it's too late is not a strategy." 135

States, businesses, and organizations need strategies for the protection of these infrastructures. Perhaps more accurately, they need a variety of strategies; securing critical network infrastructures will require both initiatives in many different areas and cooperation in many different forms.

While many of these strategies are centered at the national level, we have chosen to focus on those that necessitate international coordination. International coordination is a necessary component of any individual State's strategies for securing critical network infrastructures. We have touched on a variety of areas that might benefit from this coordination: standardization, sharing information, halting cyber attacks in progress, coordinating legal systems, and assisting developing nations.

Two of those areas may hold particular potential for successful international cooperation: information sharing and legal harmonization. Improved information sharing increases the efficacy with which States and organizations respond to challenges to the security of network systems. It enhances and enables protective actions at every level, from those of an individual securing a home network to a country securing its critical national assets. Better information gathering and dissemination can improve the ability of system administrators to defend against threats, enhance the business case for increased attention to information security, and enable risk management through insurance.

A formal international clearinghouse may be the most effective means of information sharing. Increasing international cooperation with and providing more resources for CERT/CC may help this organization to better fulfill the role of a universal clearinghouse. Otherwise, international cooperation to create a new clearinghouse may be appropriate.

An international effort that increases the ability of States to pursue prosecution of cyber criminals can build upon the benefits of information sharing. Coordinated legal efforts to prosecute cyber criminals could introduce a non-trivial element of risk for the attacker. Successful prosecution can act as a deterrent to

-

 $^{132 \}mbox{Goodman}$, 3. Much of the information in this paragraph was also taken from this source.

¹³³Goodman references Jack Goldsmith in arguing that the "international legal principles of proportionality and response-in-kind" may justify active defense measures taken by governments. Goodman, 4.

¹³⁴Goodman, 4. Much of the information in this paragraph was also taken from this source.

¹³⁵ Tenet, George J. (1998, June 24). Testimony by Director of Central Intelligence George J. Tenet Before the Senate Committee on Government Affairs. http://www.cia.gov/cia/public affairs/speeches/archives/1998/dci testimony 062498.html [2002, April 18].

prevent attacks from occurring at all; this deterrence is beneficial even if technological advances decrease the vulnerability of our networks to attack:

"If someone invented the unpickable door and window lock or the perfect burglar alarm system, no one would turn around and say: 'We don't need policy or those obsolete breaking and entry laws.' If the history of criminal activity has shown anything, it is the limits of the technology." ¹³⁶

A formal, multilateral treaty appears to be the most promising option for addressing these global security problems. While it is possible for coordination to develop without a formal accord, especially in view of the OECD precedent, the global problem is more difficult when countries have already created incompatible laws and other scattered strategies. A near-universal multilateral effort could isolate safe-havens and simplify the process of transnational investigations that include multiple States. Although the COE Cybercrime Convention is a good example of this type of effort, we would argue that the Stanford Draft Treaty is a model with greater potential for successful implementation. In particular, the Stanford Draft Treaty:

- avoids controversial topics not central to protecting infrastructures (for example: pornography, intellectual property, and counterfeiting);
- avoids specific technical detail in procedural laws, which could rapidly become outdated;
- is more readily extensible to most nations in the world;
- includes the creation of an organization, the AIIP, to provide aid to developing nations and to coordinate the efforts of the involved States.

The functions of international coordination in information sharing and prosecution could be combined; the AIIP that the Stanford Draft Treaty proposes might also be a useful home for the multilateral information clearinghouse previously described.

In today's rapidly changing, technology-driven environment, security can no longer be an afterthought. It must, instead, be carefully woven into the fabric of network infrastructures. It is not enough, however, to ensure that future iterations of these infrastructures are secure; we must secure that which already exists. The threats to critical network infrastructures and the vulnerability of those infrastructures are real and pressing.

The infrastructures are global, and the threats they face are global; the solutions must also be global. There is a need for a coordinated, sustained and institutionalized approach. Over ten years ago, the Japan Information Processing Development Center stated that "[w]e have now reached a junction when all countries must collaborate in the study of information security in the global age." ¹³⁷

The call for an international regime to secure critical network infrastructures was timely then; it is urgent now.

.

¹³⁶Schneier, Bruce. (2000). Secrets & Lies (p. 391). New York: John Wiley & Sons, Inc.

¹³⁷Cited in Kirby, Michael and Murray, Catherine A. (1993). Information Security: At Risk? In L. M. Harasim (Ed.), Global Networks: Computers and International Communication (p 167). Cambridge, MA and London: The MIT Press.

ABBREVIATIONS AND ACRONYMS

AIIP — Agency for Information Infrastructure Protection

ANSI — American National Standards Institute

http://www.ansi.org

APEC — Asia-Pacific Economic Cooperation

http://www.apecsec.org.sg

API — Application Programming Interface

APSIRC — Asia Pacific Security Incident Response Coordination

http://www.singcert.org.sg/apsirc

BIND — Berkeley Internet Name Domain

(a popular implementation of the Domain Name System (DNS) protocols used to locate

systems by name on the Internet).

CERT — Computer Emergency Response Team

CERT/CC — Computer Emergency Response Team Coordination Center

http://www.cert.org

CIAC — Computer Incident Advisory Capability (USA)

http://www.ciac.org

COE — Council of Europe

http://www.coe.int

COM — Microsoft's Component Object Model

http://www.microsoft.com/com/default.asp

CORBA — Common Object Request Broker Architecture

http://www.corba.org

CPU — Central Processing Unit

CSI Computer Security Institute http://www.gocsi.com **CSIS** Center for Strategic and International Studies http://www.csis.org **CSS** Content Scrambling System **DVD** Digital Video Disc European Union EU **FBI** Federal Bureau of Investigation (USA) http://www.fbi.gov **FIRST** Forum of Incident Response Teams http://www.first.org **G-8** Group of Eight (Canada, France, Germany, Italy, Japan, Russia, UK, USA) **ICAO** International Civil Aviation Organization http://www.icao.org **IDSS** Institute of Defense and Strategic Studies (Singapore) http://www.ntu.edu.sg/idss **IEEE** Institute for Electrical and Electronic Engineers http://www.ieee.org **IETF** Internet Engineering Task Force

IMB — International Maritime Bureau http://www.iccwbo.org/ccs/menu_imb_bureau.asp

http://www.ietf.org

ICC — International Chamber of Commerce http://www.iccwbo.org

IPv6 — Internet Protocol Version 6

ISAC — Information Sharing and Analysis Center

ISP — Internet service provider

ISO — International Organization for Standardization

http://www.iso.org

ISOC — Internet Society

http://www.isoc.org

ITU — International Telecommunication Union

http://www.itu.int

ITU-T — Telecommunication Standardization Sector,

International Telecommunication Union

http://www.itu.int/ITU-T

LEGAT — Legal Attaché (USA)

http://www.fbi.gov/contact/legat/legat.htm

MITI — Ministry for International Trade and Industry (Japan)

MLAT — Mutual Legal Assistance in Criminal Matters Treaty

http://travel.State.gov/mlat.html

NAFTA — North American Free Trade Agreement (Canada, Mexico, USA)

NIPC — National Infrastructure Protection Center (USA)

http://www.nipc.gov

International Coordination to Increase the Security of Critical Network Infrastructures

OECD

Organization for Economic Co-operation and Development http://www.oecd.org **RFC Request for Comments SEC** Securities and Exchange Commission (USA) http://www.sec.gov **SNMP** Simple Network Management Protocol SSH Secure Shell (An implementation of the Secure Shell protocol which enables encrypted access to remote systems) UK United Kingdom UN United Nations http://www.un.org US United States of America **USA** United States of America W₃C World Wide Web Consortium http://www.w3.org WEP — Wireless Encryption Protocol or Wired Equivalent Privacy protocol — Year 2000 (or the Year 2000 Bug) Y2K

REFERENCES

- Acohido, Byron. (2002, March 10). Air Force seeks better security from Microsoft. *USA Today*. http://www.usatoday.com/life/cyber/tech/2002/03/11/gilligan.htm [2002, April 28].
- American Bar Association. *International Cyber Crime Project of the ABA Privacy and Computer Crime Committee*. http://www.abanet.org/scitech/computercrime/cybercrimeproject.html [2002, April 5].
- Arbaugh, William A., et al. (2001, March 30). *Your 802.11 Wireless Network has No Clothes*. http://www.cs.umd.edu/~waa/wireless.pdf [2002, May 6].
- BBC News. (2002, April 15). *The great African internet robbery*. http://news.bbc.co.uk/hi/english/world/africa/newsid 1931000/1931120.stm [2002, April 29].
- Baker, Fred. (2000, January 25-27). *Internet Standardization and the IETF*. IP-Telecoms Interworking Workshop (Numbering, Naming, and Routing), ITU, Geneva. http://www.itu.int/ITU-T/worksem/ip-telecoms/presentations/ipw-7.ppt [2002, May 11].
- Blumenthal, U. and Wijnen, B. (1999, April). *User Based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*. Request for Comments 2574, Network Working Group, IETF. http://www.ietf.org/rfc/rfc2574.txt?number=2574 [2002, May 11].
- Bradner, Scott. (1996, October). *The Internet Standards Process Revision 3*. Request for Comments 2026, Network Working Group, IETF. http://www.ietf.org/rfc/rfc2026.txt [2002, May 11].
- Branscomb, Anne Wells. (1993). Jurisdictional Quandaries for Global Networks. In L. M. Harasim (Ed.), *Global Networks: Computers and International Communication*. Cambridge, MA and London: The MIT Press.
- Brenner, Paul and Meese, Edwin (Chairs). (2002). *Defending the American Homeland*. Washington, DC: The Heritage Foundation. http://www.heritage.org/bookstore/2002/defense/HomelandDefenseweb.pdf [2002, April 30].
- Brush, Colleen. (2001, July). Surcharge for Insecurity. *Information Security Magazine*. http://www.infosecuritymag.com/articles/july01/departments news.shtml [2002, April 27].
- Burnett, Sterling. *Opinion Editorial: Gun Lawsuits Hurt All Of Us.* National Center for Policy Analysis. http://www.ncpa.org/oped/sterling/dec1299.html [2002, May 1].
- CERT/CC. (2002, February 13). SNMP FAQ. http://www.cert.org/tech_tips/snmp_faq.html [2002, April 17].
- CERT/CC. (2002, April 5). CERT/CC Statistics 1988-2002. http://www.cert.org/stats/cert_stats.html [2002, April 29].
- CERT/CC. (2002, April 15). *CERT/CC Overview, Incident and Vulnerability Trends*. http://www.cert.org/present/cert-overview-trends [2002, May 6].
- CERT/CC. (2002, April 16). CERT Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP). http://www.cert.org/advisories/CA-2002-03.html [2002, April 17].
- Christey, Steve and Wysopal, Chris. (2002, February). *Internet Draft: Responsible Vulnerability Disclosure*. Internet Engineering Task Force. http://www.ietf.org/internet-drafts/draft-christey-wysopal-vuln-disclosure-00.txt [2002, May 6].
- Council of Europe. (2001). *Convention on Cyber crime ETS no.: 185 Explanatory Report.* http://conventions.coe.int/Treaty/en/Reports/Html/185.htm [2002, April 5].
- Cuellar, Mariano-Florentino. The Civil Aviation Analogy. In Abraham Sofaer and Seymour Goodman (Eds.), *The Transnational Dimension of Cyber Crime and Terrorism*. Stanford, CA: Hoover Institution Press, 2001.

- Federal Bureau of Investigation. About Us Legats. http://www.fbi.gov/contact/legat/legat.htm [2002, April 5].
- Federal Trade Commission. *Public Workshop: Consumer Information Security*. http://www.ftc.gov/os/2002/03/frncis.htm [2002, May 11].
- Forno, Richard. (2001, April 21). CERT: The Next Generation. The Demise of the Internet's Last Objective and "Trusted" Organization. http://www.infowarrior.org/articles/2001-03.html [2002, April 5].
- Forum of Incident Response and Security Teams. (2001, October 3). What is FIRST? http://www.first.org/about/ [2002, March 29].
- Forum of Incident Response and Security Teams. (2002, April 26). *FIRST Member Team Information*. http://www.first.org/team-info [2002, May 6].
- Gates, Bill. (2002, January 17). Trustworthy Computing. *Wired.com*. http://www.wired.com/news/business/0,1367,49826,00.html [2002, April 28].
- Gast, Matthew. (2002, April 19). *Wireless LAN Security: A Short History*. O'Reilly Network. http://www.oreillynet.com/pub/a/wireless/2002/04/19/security.html [2002, May 6].
- Goodman, Marc D. and Brenner, Susan W. (Draft 2002, March). *The Emerging Consensus on Criminal Conduct in Cyberspace*. Not yet published.
- Goodman, S. E. (2002). Toward a Treaty-Based International Regime on Cyber Crime and Terrorism. In *Transnational Cyber Security Cooperation: Challenges and Solutions*. Washington, DC: CSIS Press. Forthcoming.
- Hamre, John. (Received 2001, December 14). *Memorandum on Trans-national Collaboration in a Cyberage*. CSIS, IDSS, & Markle Foundation.
- Harrington, D. et al. (1999, April). *An Architecture for Describing SNMP Management Frameworks*. Request for Comments 2571, Network Working Group, IETF. http://www.ietf.org/rfc/rfc2571.txt?number=2571 [2002, May 11].
- Harris, Susan (Ed.). (2001, August). *The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force*. (Internet Engineering Task Force RFC 3160). http://www.ietf.org/tao.html [2002, April 18].
- International Telecommunication Union. *ITU Overview World Telecommunication Standardization Assembly*. http://www.itu.int/aboutitu/overview/wtsa.html [20002, May 6].
- International Telecommunication Union. (2002, April 4). *ITU Membership Overview*. http://www.itu.int/members/index.html [2002, April 30].
- International Telecommunication Union. (2002, April 12). *Creating Trust In Critical Network Infrastructures*. http://www.itu.int/osg/spu/ni/security/index.html [2002, April 29].
- International Telecommunication Union Technology Telecom Standardization (ITU-T). (2000, October). Alternative Approval Process for New and Revised Recommendations. (ITU-T Recommendation A-8). http://www.itu.int/dms_pub/itu-t/rec/a/T-REC-A.8-200010-I!!PDF-E.pdf [2002, May 6].
- Internet Security Systems. (2000, October 26). Serious flaw in Microsoft IIS Unicode translation. http://www.iss.net/security_center/alerts/advise68.php [2002, May 6].
- Japan Country Report. (2002). Japan Country Report. In *Transnational Cyber Security Cooperation: Challenges and Solutions*. Washington, DC: CSIS Press. Forthcoming.
- Jervis, Robert. (1978, January). Cooperation under the Security Dilemma. *World Politics*, Volume 30, Number 2.
- Jervis, Robert. (1997). System Effects: Complexity in Political and Social Life. Princeton, NJ: Princeton University Press.

- Kaspersen, Henrik. A Gate Must Either Be Open or Shut: The Council of Europe Cybercrime Convention Model. In *Transnational Cyber Security Cooperation: Challenges and Solutions*. Washington, DC: CSIS Press. Forthcoming.
- Kaspersen, H.W.K. and Lodder, A.R. (2000, April 15). *Overview of the Criminal Legislation Addressing the Phenomenon of Computer-Related Crime in the United Nations Member States*. United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (UNAFEI) Report. http://www.rechten.vu.nl/~lodder/papers/unafei.html [2002, April 10].
- Kirby, M. and Murray, Catherine A. (1993). Information Security: At Risk? In L. M. Harasim (Ed.), *Global Networks: Computers and International Communication*. Cambridge, MA and London: The MIT Press.
- Lai, Eric. (2002, March 14). *Cyber-insurance gaining popularity due to high-tech risks*. MSNBC. Reuters. http://stacks.msnbc.com/local/rtor/m23000.asp?cp1=1 [2002, April 5].
- Lemos, Robert. (2002, January 11). Microsoft's security push lacks oomph. *CNET News.com*. http://news.com.com/2100-1001-808010.html [2002, April 28].
- Litt, Robert S. and Lederman, Gordon N. (2002). Formal Bilateral Relationships as a Mechanism for Cyber Security. In *Transnational Cyber Security Cooperation: Challenges and Solution*. Washington, DC: CSIS Press. Forthcoming.
- Luciano, Elizabeth. (2002, April 4). *UMass computer scientist offers a new way to track Internet vandals*. http://www.eurekalert.org/pub_releases/2002-04/uoma-ucs040402.php [2002, April 18].
- Lukasik, Stephen. (2001, October). *Responding to Cyber Threats: The International Dimension*. Stanford University's Consortium for Research on Information Security and Policy & the Georgia Tech Information Security Center.
- Lukasik, Stephen et al. *Strategies for Protecting National Infrastructures Against Cyber Attack*. London: International Institute for Strategic Studies. Forthcoming as an Adelphi Paper.
- Magnusson, Paul. (2002, April 1). The Highest Court You've Never Heard Of. Business Week.
- Martin, Brian a.k.a. Jericho. (2001, April 19). Cashing in on Vaporware. http://www.attrition.org/security/rant/z/jericho.007.html [2002, April 5].
- Ministry of Economy, Trade, and Industry. (2001, September 3). *OECD Workshop: "Information Security in a Networked World"*. http://www.meti.go.jp/policy/netsecurity/OECDwrkshpAgenda.htm [2002, May 11].
- Mukundan, P. (2002). Laying the Foundations for a Cyber-Secure World. In *Transnational Cyber Security Cooperation: Challenges and Solutions*. Washington, DC: CSIS Press. Forthcoming.
- National Cyber crime Training Partnership. (2000, March). *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet*. http://www.nctp.org/append10.html [2002, April 5].
- National Infrastructure Protection Center (NIPC). *Information Sharing Outreach*. http://www.nipc.gov/infosharing/infosharing.htm [2002, March 28].
- National Infrastructure Protection Center. (1998, May 22). The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. http://www.nipc.gov/about/pdd63.htm [2002, April 3].
- Organization for Economic Cooperation and Development. (1997, July 1). *Guidelines for the Security of Information Systems*. http://www1.oecd.org/dsti/sti/it/secur/prod/e secur.htm [24 April 2002].
- Organization for Economic Cooperation and Development. (1997). *Review of 1992 OECD Guidelines for the Security of Information Systems*. http://www1.oecd.org/dsti/sti/it/secur/prod/reg97-2.htm [2002, May 10].
- Pescatore, John. (2001, September 19). *Nimda Worm Shows You Can't Always Patch Fast Enough*. Gartner Research. http://www4.gartner.com/DisplayDocument?id=340962&acsFlg=accessBought [2002, April 28].

- Powell, Robert. (1991, December). Absolute and Relative Gains in International Relations Theory. *American Political Science Review*, Volume 85.
- Power, Richard. (2002, Spring). 2002 CSI/FBI Computer Crime and Security Survey. *Computer Security Issues & Trends*. Computer Security Institute. http://www.gocsi.com/press/20020407.html [2002, April 17].
- President's Commission on Critical Infrastructure Protection. (1997, October). *Critical Foundations:*Protecting America's Infrastructures The Report of the President's Commission on Critical
 Infrastructure Protection. (GPO No. 040-000-00699-1). Washington, DC: U.S. Government Printing
 Office. http://www.info-sec.com/pccip/pccip2/report index.html [2002, April 18].
- Radcliff, Deborah. (2000, August 21). Got Cyber Insurance? *Computerworld*. http://www.computerworld.com/managementtopics/ebusiness/story/0,10801,48721,00.html [2002, May 7].
- Richenaker, Gary. (2001, December 18). Report of IP-Telecoms Interworking Workshop (Numbering, Naming, Addressing and Routing) ITU, Geneva 25-27 January 2000. http://www.itu.int/ITU-T/worksem/ip-telecoms/index.html
- Sager, Ira and Greene, Jay. (2002, March 18). Commentary: The Best Way to Make Software Secure: Liability. *Business Week Online*. http://www.businessweek.com/magazine/content/02_11/b3774071.htm [May 9, 2002].
- Schneider, Fred B. (Ed.). (1999). Trust in Cyberspace. Washington, DC: National Academy Press.
- Schneier, Bruce. (2000). Secrets & Lies. New York: John Wiley & Sons, Inc.
- Schneier, Bruce. (2001, February). Schneier on Security: The Insurance Takeover. *Information Security Magazine*. http://www.infosecuritymag.com/articles/february01/columns_sos.shtml [2002, April 4].
- Schneier, Bruce. (2001, August 13). *Declaration of Bruce Schneier in Felten v. RIAA*. Electronic Frontier Foundation. http://www.eff.org/IP/DMCA/Felten_v_RIAA/20010813_schneier_decl.html [2002, May 6].
- Slashdot.org. (2000, October). *CERT and Vulnerability Disclosure*. http://slashdot.org/articles/00/10/08/1815211.shtml [2002, April 4]
- Snoeren, Alex C. et al. (2001, August). Hash-Based IP Traceback. *Proceedings of the ACM SIGCOMM 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*. http://nms.lcs.mit.edu/~snoeren/papers/spie-sigcomm.pdf [2002, May 6].
- Sofaer, Abraham D. and Goodman, Seymour E. (2000, August). A Proposal for an International Convention on Cyber Crime and Terrorism. The Hoover Institution: Stanford, CA
- Sofaer, Grove, and Wilson. (2001). Draft International Convention to Enhance Protection from Cyber Crime and Terrorism. In A. D. Sofaer, and Seymour E. Goodman (Ed.), *The Transnational Dimension of Cyber Crimes and Terrorism*: The Hoover Institution on War, Revolution and Peace.
- Tenet, George J. (1998, June 24). *Testimony by Director of Central Intelligence George J. Tenet Before the Senate Committee on Government Affairs*. http://www.cia.gov/cia/public_affairs/speeches/archives/1998/dci_testimony_062498.html [2002, April 18].
- The Canadian Trade Commissioner Service. (2000). *EXTUS Trade Mission Globetech Sector Information Technology in Washington*. http://www.infoexport.gc.ca/mission/globetech/tech in wash-e.asp [2002, May 6].
- Trusted Computing Platform Alliance. http://www.trustedpc.org [24 April, 2002].
- United States Department of Justice. (1997, October). *United States Attorneys' Manual*. http://www.usdoj.gov/usao/eousa/foia reading room/usam/index.htm [2002, April 4].

- U.S. Department of State. *Mutual Legal Assistance in Criminal Matters Treaties (MLATs) and Other Agreements*. http://www.travel.state.gov/mlat.html [2002, April 5].
- U.S. Senate Permanent Subcommittee on Investigations. (1999, June 5). *Security in Cyberspace*. http://www.fas.org/irp/congress/1996_hr/s960605b.htm [2002, April 30].
- Vatis, M. (2002). International Cyber Security Cooperation: Informal Bilateral Models. In *Transnational Cyber Security Cooperation: Challenges and Solution*. Washington, DC: CSIS Press. Forthcoming.
- Wearden, Graeme. (2002, January 23). DoS attack shuts down ISP Cloud Nine. *ZDNet (UK)*. http://zdnet.com.com/2100-1105-820708.html [2002, April 5].
- Wilcox, Joe. (2002, February 12). Can MS juggle privacy and security? *ZDNet News*. http://zdnet.com.com/2100-1104-835802.html [2002, April 28].
- Wipro, Ltd. *Utilities Case Study #23*. http://www.wipro.com/itservices/industries/utilities/utilcasestudy23.htm [2002, April 30].