Visions of the Information Society

Network security:
Protecting our critical infrastructures

This paper was prepared by Professor Seymour E. Goodman, Pam Hassebroek, and Professor Hans Klein, Georgia Institute of Technology (United States). “Network Security: Protecting our critical infrastructures” forms part of the Visions of the Information Society project managed by Lara Srivastava <lara.srivastava@itu.int>, Policy Analyst in the Strategy and Policy Unit of the International Telecommunication Union (ITU). More information can be found at http://www.itu.int/visions. The views expressed in this report are those of the authors and do not necessarily reflect the opinion of ITU or its membership.

Table of contents

1 Introduction: The nature of the problem

Over the last century and a half, several new technology-based infrastructures have been created. They have been developed and used so extensively that they now partially characterize modern societies. Four of the most important infrastructures are built up around the core technologies of the internal combustion engine, aircraft, space flight, and radio and television. "Cyberspace"—defined as the Internet and other wide area networks based on computing and other information technologies (IT)—seems on its way towards becoming the latest such infrastructure. In little more than 30 years, cyberspace has become the locus of much value, notably in terms of information and money. Cyberspace can further be considered a means of passage, enabling extended personal and organizational presences and interactions. For a number of Organisation for Economic Cooperation and Development (OECD) member countries and global economic sectors, cyberspace has also become a locus for many systems that control and manage other more traditional infrastructures, such as those for banking and finance, emergency services, energy delivery, and many transportation and military systems. These computer communications networks are the underlying technological bases that will enable any and all "visions of the information society."

1.1 Cyberspace is complex

Cyberspace now consists of a collection of rapidly growing networks and systems, systems that are large, diverse, complex, interconnected, and fragmented. Much of it has been built piecemeal by many different people and organizations using a wide assortment of information technologies, and with a wide assortment of functionalities in mind. The interoperability of hardware and software along with a few basic protocols permit an extraordinary degree of access and connectivity.

To get a sense of the growth of cyberspace, consider the recent international expansion of the Internet, by far the largest of these networks. By 1984—almost half of the time since the 1969 birth of the ARPANET under the US Department of Defense—the entire network consisted of about 1,000 host computers located in fewer than a half dozen North Atlantic Treaty Organisation (NATO) member countries. By 1989, only a few years after much of the network migrated out of the Department of Defense and became the Internet, the count had risen to around 20 countries and 100,000 hosts. But the vast majority of those hosts were still in the United States.

Since then international growth has been explosive. There are now over 200 countries and a few other entities[1] with full TCP/IP connectivity. Worldwide growth has been 50–100 per cent per year, and much higher in some years in many countries. More of the Internet is now outside of the United States than inside. As of early 2002, there were tens of millions of host computers and perhaps at least a half billion users worldwide, with something approaching a quarter of the users located outside of the OECD countries. Improving technology, declining cost, and the demographics of the world's under-30 population are favoring growth beyond the OECD. For example, within the last 7 to 8 years, the user populations of China and India have grown from almost negligible numbers to at least 50,000,000 and 10,000,000 respectively. Other countries, e.g. Turkey and Pakistan, each generated a million or more users within one to three years of the start of public access.[2]

Over the course of the last decade or two, several truly global infrastructures, including banking and finance and civil aviation, have become pervasively dependent on computer-telecommunications systems for much of their functionality and efficiency. They are so dependent on these systems that they are probably no longer effectively able to revert to extensive manual systems without severe and crippling loss of capabilities.

The widespread connectivity and functionality, the emphasis placed on providing extensive and inexpensive access—as well as the other opportunities permitted by these networks—have attracted a large, diverse, fragmented, rapidly growing, set of public and private constituents and stakeholders. These include the infrastructure owners, operators, suppliers, organizational and individual users, and governments in many capacities. There is an extensive and rapidly growing use of and dependence on these infrastructures by these constituents.

1.2 Cyberspace is vulnerable

The infrastructures of cyberspace are vulnerable due to three kinds of failure: complexity, accident, and hostile intent. Very little of it was designed or implemented with assurance or security as primary considerations.[3] Bad things can be done either via the network infrastructures or to the infrastructures

themselves. These bad things can be characterized by a lot of "D" words: destroy, damage, deny, delay, deceive, disrupt, distort, degrade, disable, divulge, disconnect, and disguise. Cyber attacks under these categories are reported almost daily in the news media. Hundreds of millions of people now appreciate a cyber context for terms like "viruses", "denial of service", "privacy", "worms", "warfare", "fraud", and "crime" more generally.

We lack a comprehensive understanding of these vulnerabilities—largely because of the extraordinary complexities of many of the problems, and perhaps from too little effort to acquire this understanding. But there is ample evidence that vulnerabilities are there: examples of all three kinds of failure abound, and vulnerabilities are found almost every time people seriously look for them (e.g. via "Red Teams"). Under the circumstances, it is remarkable that we have had so few extended and crippling failures so far.

Threats to network infrastructures are potentially extensive not only as their value increases in terms of the infrastructures themselves, the value of hosted services, and the value of what is located on them, but also because of their widespread and low-cost access. The connectivity of the networks gives rise to a form of long, nonlinear reach for all kinds of attackers that is not present for more traditional forms of infrastructure attacks, e.g. bombs against physical transportation systems. Dependence on some of the IT-based infrastructures in several countries is such that serious national consequences could result from the exploitation of their vulnerabilities.

Thus it is not surprising that these infrastructures are attracting a wide range of malevolent activity ranging from a great deal of long range vandalism, to many forms of more serious crimes, to prospective forms of terrorism, to nation-versus-nation conflict. Attacks may be directed at parts of the information infrastructure itself,[4] or through the networks against other targets that have a presence in this medium. Criminals and terrorists may also value the networks as assets to support their own activities, e.g. for inexpensive, effective communications or as a source for intelligence gathering.[5] Virtually every connected country can serve as a base for any number of attackers, who are motivated, and who can readily acquire access and technical capabilities to cause harm to others.

Attacks so far have been limited. While in some network attacks the value of losses is in the hundreds of millions, damage so far is seen as tolerable. Many believe that it is only a matter of time before all sorts of malevolent people are going to find those network vulnerabilities and exploit them through prolonged, multifaceted, coordinated attacks producing serious consequences. Thus, prudence dictates better protection against accidents and attacks before things get much worse. Is this a domain where "a stitch in time may save nine", and one where government and industry can get out ahead of a problem before it becomes insufferable? However, since one unprotected system renders the entire network vulnerable, cooperation between all governments and their constituents is required for a safer network environment. And, all realizations of "visions of the information society" are going to be severely limited if the people in that society do not trust or feel secure with the underlying infrastructures.

Strategic defence options[6]

> "Security is a process, not a product."[7]

Faced with the technical possibility of disruption of critical infrastructures in ways that could have serious consequences to their economies and potentially result in loss of life, governments should be expected to plan and implement prudent defences. Policies directed to protecting infrastructures will, in the majority of countries, require that there be a clear logic relating the perceived states of infrastructure vulnerability to the desired endpoints such defensive policies are intended to achieve. This will require that each country identify those infrastructures, and their interdependencies that are critical to its survival and to its social and economic well-being.

Absolute defence against cyber attack has rarely, if ever, been achieved in a large complex, geographically distributed, network. The complexities of such systems and modes of attack are such that we do not know precisely how to assess how secure they are, and this lack of understanding forces defenders to protect themselves in overlapping ways and in multiple stages.

Protecting infrastructure systems arguably involves five coupled stages. First, it is necessary to attempt to deter potential attackers. Second, if attacked, the need is to thwart the attack and to prevent damage. Third, since success cannot be guaranteed in either preventing or thwarting an attack, the next stage is to limit the

damage as much as possible. Fourth, having sustained some level of damage from an attack, the defender must reconstitute the pre-attack state of affairs. Finally, since changing technology and incentives to attack influence both offence and defence, the final step is for the defender to learn from failure in order to improve performance, just as attackers will learn from their failures.[8] We will discuss these stages in more detail in the sections that follow.

The more specific defences to be discussed may be usefully partitioned into two forms: passive and active. *Passive defence* essentially consists in target hardening. Examples include internal use of various technologies and products, such as firewalls and cryptography, and procedures to protect the assets owned by an individual or organization. Some forms of passive defence may be dynamic, e.g. stopping an attack in progress by closing vulnerability in real time. But, by definition, passive defence does not impose serious risk or penalty on the attacker. With only passive defensive measures, the attacker is free to continue to assault the target. Given the vulnerabilities of most cyber systems and the low cost of most attacks, a skilled and determined attacker is likely to eventually succeed if he can keep trying safely. *Active defence*, in contrast, imposes some risk or penalty on the attacker. Risk or penalty may include identification and exposure, investigation and prosecution, or pre-emptive or counter attacks of various sorts.

There will be trade-offs between the various courses of action suggested by this conceptual structure. Preventing or thwarting attacks can be costly. This activity may also incur losses through reduced system performance. However, the greater the success in limiting damage, the less will be the amount of damage to be repaired. If limiting damage is difficult, it is better to invest in efforts to assist in reconstitution. Damage limitation can be viewed on two time scales. Plans can be made to limit the damage from a single attack, or to minimize losses from multiple attacks over time. There will be other trade-offs, e.g. between detailed and potentially costly scrutiny of individual transactions and that of waiting to identify and punish attackers over the longer term.

Since an infrastructure system is typically a mix of public and private ownership, the various 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 economies and national security, and maintaining law and order.

1.3 Preventing an attack

There are at least three ways to prevent an attack, and all three are ultimately forms of active defence. One is to *deter* the attacker by having a demonstrated capability to punish the attacker. This implies that the attacker understands the risk of being identified and located; that the defender is seen as credible in a resolve to punish, and that the “cost” of punishing is acceptable to the defender. A simple situation is when the attacker suffers a large “front end” loss through discovery during the probe phase and the defender can accomplish that discovery cheaply. When the cost to the defender to punish is less than the loss that can be caused by the attacker, there will clearly be an incentive to develop ways of discovering attackers. But the more common situation is when the relatively high costs of legal prosecution of a single attacker are returned in reduced losses over the longer term.

Deterring criminal actions requires some amount of international legal machinery such as common definitions of criminal actions, standards for the collection of forensic evidence, extradition agreements, and the like. Deterring State attackers requires less in the way of legal procedures, but requires the defender to have a national policy that recognizes information attacks as attacks under the United Nations Charter that justify self-defence and constitute threats to peace. Costs of deterrence as seen by a government will differ from those seen by a private system owner in magnitude and cost-benefit expectations. National expenditures for a prompt capability to respond to attacks on the State include the correlation of intrusion events, the collection and dissemination of attack profiles and warnings, and the costs of participation in international organizations and joint responses.

A second way to prevent an attack is through establishing cyber attacks as *unacceptable behaviour* among the community of nations. This can be through formal arms control agreement, or it can be based on domestic laws and international agreements designed to protect privacy, property rights, and other generally accepted areas of mutual interest. Again, there is the implication that violators can be subject to sanctions

including social disapproval, civil or criminal penalties, or revocation of rights of access and use, a cyber equivalent of exile.

A third way to prevent an attack is to *pre-empt* the attacker in a way that results in abandoning the attack. This implies a great deal by way of national surveillance capability to be able to provide strategic warning. So stealthy are cyber attacks, so widespread is the ability to plan and launch them, so inexpensive are the tools of attack, and so lacking are the indicators of cyber attacks that pre-emption would not appear to be a practical option at this point. But should responsible norms of behavior in cyberspace become better established, the detection and identification of abnormal behavior may become easier.

Note that for the most part preventing cyber attacks is the responsibility of sovereign States, such as in the operation of law enforcement agencies, threatening the use of various degrees of force, and maintaining a global surveillance capability to discover the intentions of potential adversaries. In many countries of the world, the pursuit of these active defences by private entities would be of doubtful legality.

1.4 Thwarting an attack

While preventing attack is largely based on government authority and responsibility, the detailed knowledge needed to thwart an attack on a cyber system to prevent damage rests primarily with its owner. The least complicated case is where the system owner acts individually. Not only must the owner be concerned with defence from outsiders, but also needs to recognize that not all authorized users of the system may have the owner's interests at heart. There are many ways of defending systems against cyber attack, and some minimal number must probably be employed for the owner to demonstrate due diligence.

Thus, techniques such as requiring authorization to enter, monitoring and recording the use of the system to detect unauthorized activities, periodic checking on the integrity of critical software, and establishing and enforcing policies governing system security and responses to unexpected event will be necessary. Owners can limit unauthorized activities through compartmenting information within the system and maintaining need-to-know discipline. Owners can provide themselves substantially more rights to monitor inside users by covering access through contractual terms with employees and vendors.

Considerably more potential for protecting systems is possible when system owners work cooperatively for their mutual benefit. In doing this, there is a trade-off between gaining from the collective knowledge of a larger group and the potential for loss due to the possibility of greater access to one's systems and information. With the presumption that adequate controls govern cooperative defence, there are opportunities for pooling information of many types: vulnerability, rate and severity of attacks being experienced by others, attack profiles and suspected attackers. There is also the possibility for pooling capabilities in security research and development (R&D), penetration testing, determining security standards and industry best practices; and contributing to the establishment of educational and training curricula and professional security personnel certification.

Another approach to thwarting an attacker's goals is to build systems with degrees of intrusion-tolerance. These would have as their intent to limit the effectiveness of single intruders through such architectural approaches as distributed control, multiple redundant systems with voting, incorporation of air gaps, automated and manual monitoring of critical operations, and the like. Other approaches would include increasing the number of potential target points on which the attacker can expend resources, construction of virtual decoy facilities with which to distract attackers, and internal compartmentalization to contain damage. These have obvious parallels to common defensive techniques that are ingrained in military planning but are not typically part of the repertoire of computer system designers and administrators.

Almost all of these forms of defence are passive, and would be the responsibility of the system owners and operators. In different parts of the world, and for different infrastructures, these may be either governments or private entities. Some of this, e.g. a cyber attack warning system, might be under the purview of national or international bodies. The most active form of defence in this phase is dealing with the insider threat, where an employer may be able to impose serious risk on the attacker. Although the fraction is dropping, insider threats still probably account for at least half of the seriously damaging computer crimes in most of the world.

1.5 Limiting damage during a successful attack

The central idea of this strategic objective is to limit damage in the trans-attack period by constructing an “incident management” system. The premised technical capability is the ability of the defender to audit system operation, to be able to detect an attack underway, and to take steps in real-time to limit the extent of the damage. “Defender” can apply to the company level, the industry level, or the national level.

Damage limitation implies, beyond having attack “templates” to enable recognition that an attack is under way, the linking of system operation centers to higher-level analysis centers for situation awareness and attack assessment. This also implies having pre-established response options at the company, industry, or national level.

Several kinds of responses are possible. Adaptive defence allows a defender to increase levels of defence, such as calling for re-authentication of all users, or those currently undertaking critical functions or accessing critical information, putting critical transactions in “quarantine” until they can be more thoroughly scrutinized, backing-up system status, providing real-time warning to other systems, and increasing the collection of forensic evidence.

Other responses might include undertaking active defence measures such as tracing at the packet, message, or session level, blocking traffic from or to attacker locations, and instituting legal actions to search and seize attacking computers. Such aggressive measures will generally be beyond the competence and jurisdiction of any but national authorities and thus such responses are likely to require broad determinations of national security. On the other hand, private entities acting either alone or cooperatively can undertake some of these responses, subject to terms of their contractual agreements and regulatory limits on discriminatory network behavior.

Damage limitation can also include an ability to use preplanned redundancy and the establishment of a priority structure to dynamically reconfigure a system and reallocate load. This implies a capability to do system simulations in near-real time and to have established and rehearsed response plans. Another possible approach may be to exploit local redundancy to support locally suitable responses, e.g. handing off load to other sites in accordance with prior agreements to provide specified degrees of backup.

Such near-real time responses, by their nature, reveal a capability to monitor, track, identify, and take action against attackers. The decision to employ them requires weighing the value of a response in each case against the long-term costs of revealing those capabilities and the nature and effectiveness of the adaptive responses.

1.6 Reconstituting after an attack

Short-term reconstitution is the set of first steps taken to meet the most urgent threats to life and property. They include assessing damage and implementing an appropriate recovery plan. Systems are restored from backups where possible, and residual resources may have to be rationed. It is possible that additional capacity can be generated as facilities that are idle or in maintenance are brought on line. Online status reporting, dispatching of emergency personnel and repair equipment, notification of users of possibly lost transactions, an ability to adjust plans in near-real time, and procedures for secure emergency communication will be required.

Long-term reconstitution of facilities and information may also be required, especially where physical damage has occurred. This will involve the identification and stockpiling of long-lead items. Managing such risks will require industry-wide planning, such as to share surviving capacity, to insure against loss, and to spread risk across insurers. The collection of loss data will enable both operators and insurers to manage risks most effectively. In the case of major loss, governments are likely to have an underwriting role as well.

What is needed in all these situations is a healthy dose of worst-case planning. After-the-fact analysis of system failures from natural events and lower-level attacks will aid in this process. Long-term reconstitution includes the ability to use actual events to identify failure modes and fixes. This process must be a continuing one to address changing technical capabilities and evolving circumstances.

Reconstitution responsibilities involve mostly passive measures that will fall heavily on infrastructure owners and operators. But facilitating the generation of emergency capacity and playing a role in underwriting recovery are likely to involve government authorities and use of public assets.

1.7 Improving defender performance

A current management paradigm asserts that organizations must learn from experience. Even under the best of circumstances, events often unfold unpredictably. Social and technological change may also diminish an organization's present effectiveness. Recognizing this, there are two responses. The first response is to recognize the possibility that the network system could fail in several ways. Initial design of new systems, or upgrades of existing systems, should include thorough analysis to identify potential flaws an attacker could exploit.

In this regard, system design must have an explicitly defensive aspect, where models of attackers and their strategies and tactics are established and where tools for the collection of forensic data are provided. An analogy is the design of a military combat system. Not only must a system meet its functional objectives, but its defence in the face of hostile action is addressed at the beginning of the design process, not, as is often the case in commercial systems, the end of the process or even reactively. Information about the defence of the system should be concealed from potential attackers and the system should be designed to give unsuccessful attackers as little information as possible on which to develop improved attacks. As a second response toward improving effectiveness, during the development process, and after deployment, systems should be subject to independent penetration testing.

Post-attack analysis of intrusion attempts, whether the attack was successful or not, is critical for a learning organization. While failure analysis is normal in areas such as transportation, power, and structural failure, it is less common in the case of information systems where failures are more difficult to diagnose and where forensic evidence is more difficult to collect. Such data as are collected must be analysed, not only to assess damage, but also to thwart a recurrence of that attack and to address possible inadequacies in forensic data collection. While this may smack of locking the barn door after the horse has been stolen, if successful, the same attacker or others may repeat attacks, and hence there is ample opportunity for learning in the large.

Forms of international cooperation[9]

Some of the defence strategies described in Section 2 cannot be effectively accomplished without international cooperation. To universally recognize cyber attacks as unacceptable behavior, including common definitions of criminal actions, requires some amount of international legal machinery. The creation of international standards for the collection of forensic evidence, extradition agreements, and the like includes a host of coordinating efforts. A global intelligence capability and cyber attack warning system likewise requires cooperation to be effective and generally beneficial.

We recognize that any international coordination is especially complicated with respect to network systems security. Not only are information systems technically complex, they also involve a number of national regulatory and law enforcement bodies, such as trade, telecommunications, intelligence, and defence. And internally, national security plans require cooperation between government agencies as well as non-governmental organizations.

Considering this complexity, we identify five areas requiring international cooperation where we see reasonable expectation for achievement: international standards, information sharing, halting attacks in progress, harmonizing legal systems, and assistance to developing countries. For each area, we examine current efforts and suggest where new or expanded efforts could be beneficial.

1.8 International standards

Standards in network components have provided both the possibility for creating networks and the potential for using them to wreak havoc. However, the misuse of systems, whether purposeful or accidental, can be minimized by the development of standards for secure software and standards for secure network systems. Standards can be achieved by both formal and informal means. Standards may be formally developed by a standards-setting body and officially recognized as such. Informally, standards are achieved by common practices and the use of common products. For example, a certain communication protocol may be an example of the former, while the Microsoft Windows operating system is an example of the latter. Because of the pervasiveness of each of these methods, each demonstrates an effective propagation means for network "malware".[10] Whether the security flaw exists in code because of an "official" standard or in a commonly used software application, the vulnerability is the same. By the same token, each method can also provide the opportunity for increasing network security.

1.8.1 The standards development process

Various individuals and groups produce at various times the standards and protocols that allow the functioning and interconnection of networks in cyberspace. For example, the information flowing over lines built to standards of the International Telecommunication Union (ITU) may follow "standards" developed by private companies, governments, academic institutions, collaborating free agents, and organizations that have no official legal authority (such as the World Wide Web Consortium (W3C)). A wide variety of other official and semi-official standards bodies also influence standards-setting, one being the Internet Engineering Task Force (IETF).

The IETF has a rather unorthodox structure for a standards body in that it "is a loosely self-organized group of people who contribute to the engineering and evolution of Internet technologies. It is the principal body engaged in the development of new Internet standard specifications. 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."[11]

In spite of their very different approaches to defining standards, the IETF and ITU collaborate and have even developed standards jointly.[12] The IETF is a unit of the Internet Society (ISOC), and as such is considered part of an ITU Sector Member. Internet standards efforts through the IETF and others, while immensely useful, have developed largely ad hoc and without a design plan that incorporates security. However, as the security of any network depends directly on the underlying security of its standards, flaws have—predictably—surfaced. As an example, several standard Internet services such as the Telnet protocol, which are defined as IETF's 'Request for Comments' (RFC) – RFC0318 and RFC0435—send passwords as plain text that hackers can intercept with sniffer programs. And, as we discuss in Section 3.3 below, the IP protocol itself offers inefficient means of tracing malicious packets back to their source.

Because of the increasing volume of security breaches and associated financial losses, such Internet insecurities are being addressed. However, the creation of secure software leading to a secure cyberspace requires a commitment on the part of all software developers now and in the future to write code that protects against its misuse. Microsoft has announced its commitment to a focus on security in their products, which many of the world's users employ. On January 15, 2002, Microsoft Chairman Bill Gates sent an e-mail urging employees to make their software "as reliable and trustworthy as electric, water, and telephone service"[13]. Expectations rise with such an announcement, but this task is not an easy one and constant attention to security will be required as security flaws in these and other complex computer systems are revealed.

Improving the security of standards affecting cyberspace will require encouraging all organizations that develop standards to include security as a design rationale. It will also require promoting awareness among users such that security will be one of the principal criteria for choosing products with competing standards.

1.8.2 Open source security standards

Software security standards have been achieved either through official standards-setting bodies or through development of software products that are commonly used. What role, if any, does the open-source community play in security standards setting?

The effect on security of open-source software, and on security standards through its use, is a major debate in the security community. However, a number of prominent experts believe that it has the potential to be more secure than its proprietary counterparts [14].

Open-source software (OSS) includes free and non-proprietary software, as well as software developed in open collaboration to achieve marketable product subsequently licensed for profit. Supporters of open-source software claim that their development approach is inherently more secure than that of proprietary software because a broad community of programmers tests OSS [15]. Security holes are thus more quickly discovered than in proprietary products, which rely on a small pool of in-house testers. Proprietary software receives an equivalent public testing only after being implemented — and then the people trying to break in are authentic "bad guys" intent on doing real harm. The use of proprietary software without source code may actually create security risks, since it makes the detection of malware difficult.

Critics of OSS, on the other hand, note that it is slower to be upgraded. It is often argued, as well, that if all eyes can see the code, then malicious eyes cannot be excluded through the background check process so often used by proprietary software development companies. Peter Neumann, a security and networking

expert at SRI International, in Menlo Park, Calif., believes that open source is not inherently more secure. “Unless there's a great deal of discipline underlying the development, there's no difference in the security [of proprietary and open-source software]. If everyone has the same bad skills, all the eyeballs in the world won't help you. Unless there's discipline, you still come up with garbage” [16].

Neither the proprietary nor the OSS approach is without flaws. While the security weaknesses of some proprietary products (e.g. Microsoft) are well known, the weaknesses in others may be less publicized. For example, in 2002 the Slapper worm successfully penetrated servers running the OpenSSL Toolkit. [17]

Although it does not appear to be a major source of security software, the importance of OSS software is growing. Open-source software, the hardware that runs it, and services to support such software accounted for only 0.5 per cent to 1 per cent of commercial spending in the computer-security market as of year-end 2002. But that is an increase from zero only two years earlier [18]. However, since much open-source software is available free, spending in the marketplace is not an accurate measure of its level of implementation. Open-source software, by its nature, tends to be highly specialized to specific, detailed functions and is actually widely implemented [19].

As an example, Kerberos is a tried and true open source security standard that was developed at MIT in the late 1980s. The Kerberos protocol combines passwords and symmetric key encryption to authenticate users and protect communications in network connection and has been included in the Microsoft Windows 2000 operating system. As an integral part of a proprietary product, this Kerberos adoption now offers the robust security standard the potential to reach an even wider user and developer audience [20].

1.8.3 Incentives to establish security standards

For any number of reasons, many users continue to interconnect their unsecured systems in cyberspace in spite of well-documented risk to their personal and organizational assets. And cyberspace is only as safe as is the most vulnerable system connected. In view of the fact that we now believe that critical infrastructures are at risk, it is in the best interest of all nations to encourage their citizens to secure their network activities.

A variety of incentives are available to encourage the establishment and use of standards designed for network security. As examples, national governments can influence standards adoption by providing security guidelines and purchasing rules, and by introducing tax incentives and other regulations.

To encourage increased security in its member nations, the Organisation for Economic Cooperation and Development (OECD) Information, Computer and Communications Policy (ICCP) Committee developed the OECD Guidelines for the Security of Information Systems (“Guidelines”) as a model for national policies. The committee that developed the Guidelines was made up of a group of experts drawn from government, industry, and academia. The OECD member countries adopted the Guidelines on 26 November 1992.[21] They were subsequently revised and adopted as a Recommendation of the OECD Council at its 1037th Session on 25 July 2002. One of the goals of the work is the protection of individuals and organizations from harm resulting from failures of security. “As a user of information systems and networks, government has a responsibility to ensure that its use is consistent with the Guidelines, in particular the ethics and democracy principles, and thus contributes to a secure global system”.[22] The Guidelines, while voluntary, are used in many countries for study and to act as a baseline for policy development.

Government purchasing behaviour can also influence standards development and adoption. The Ministry of International Trade and Industry (MITI) security initiative in Japan is an example of an attempt to influence the market through a security initiative in a non-coercive manner similar to the methods used with the OECD Guidelines. The MITI standards, established primarily to motivate action to prevent security breaches,[23] do not have legal force in Japan, but they do constrain the purchasing decisions of government agencies. Since government purchases constitute a large part of the market, industry either has to comply with the standard or be shut out of the public procurement market. This provides an effective mechanism, an economic incentive, to realize the implementation of many standards.

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.[24] Thus, economic incentives again influence the adoption of security standards.

Insurance companies can play a role here also. Lower premiums can be charged to companies that secure their systems, while higher prices may be charged to those that do not. For example, one insurance company

charges 10 to 15 percent higher premiums to firms that use a known insecure proprietary web server.[25] This action moves risk to an operating cost, thereby providing and incentive for changes in behavior to address network security.

A similar economic incentive for better network security is the potential for assuming liability. Some believe that developers should be held liable for software that has not been properly designed and tested before being made public. On January 8, 2002, the US National Academy of Sciences proposed that lawmakers consider legislation that would end software companies' protection from product liability lawsuits. Software developers have heretofore 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."[26]

However, a Korean civic group is considering just such legal action against Microsoft, blaming the company for the January 2003 SQL "Slammer" virus. The group says it plans to build its case on a product liability law recently enacted that holds manufacturers responsible for physical and property damage caused by flaws in its products.[27] Liability is one way of forcing secure software. Can standards for secure software be developed so that all software is designed and written with the same safeguards?

Trust on the part of consumers and constituents is a valuable asset for a business organization as well as a regulatory agency. Various forms of network surveillance along with failures in online transactions have created distrust in the privacy and security of our networked systems. The 2001 World Trade Center and Pentagon terrorist attacks in the United States have added a new level of fear to the global community. There is an incentive now to revitalize the order and trust that is engendered by the stability and reliability of communications systems. Standardization in security design for network transactions can help.

Such standards also allow efficient production. If a variety of different design standards are employed, manufacturers are forced to make different products for different markets, thus diminishing economies of scale.[28] Different regulatory standards in different jurisdictions, along with the costs associated with divergent standards, can lead to inefficiencies. Standards considered in this perspective provide yet another economic incentive to improve security, along with their role in reducing costs in recovering from cyberspace attacks.

International standardization is increasingly important "because only global solutions can satisfy the needs of geographically dispersed and vertically integrated industries. [N]ew mechanisms are needed to facilitate global collaboration on standardization questions at early stages of technological innovation."[29] It is at early stages that security issues should be investigated and provided for in new technologies. Poor design has caused failure in new technologies; and certainly poor design and engineering has caused much frustration.

1.8.4 International alliance for security standards

Program and product design that allows deliberate attack on network systems carries potential for heavy financial loss. An international alliance for security standards could assure and insure technology design for network security. An important part of introducing standards in system design is the necessary step of assessing conformity to specific standards.[30] A national and international system for certifying security, such as the globally recognized ISO 9000 series in manufacturing, could serve as an important step to preventing security failures.

The addition of this mission to an existing international organization is worthy of consideration. ITU is responsible for standardization of international telecommunications including radiocommunications, as well as the harmonization of national policies. ITU develops standards to foster the interconnection of telecommunication systems on a worldwide scale regardless of the type of technology used.

ITU also recommends practices for the prevention of interference among transmissions in international spaces. To the extent that such spaces can be made secure, the convention is already in place to achieve such a standard. However, there are further needs for international standards and recommended practices in security policy generally. Since malevolent code can be routed through nodes in countries without standards or policies, such countries can offer an attractive launching point for criminal activities. Cyber security awareness should be fostered so that consensus among nations can be achieved at least in realizing the dangers of doing nothing. Formal agreements among States that have achieved standard security laws and

procedures are rendered less effective when an attack involves a nation without such protections. Where resources are scarce for creating security policy from within a country, a standard policy model can be developed and offered that can serve to prevent attacks and preserve system functions to the extent possible. An individual government would then be responsible for laws and procedures that insure the enforcement of any policy that is established. We discuss efforts to aid developing countries in Section 3.5.

1.9 Information sharing

Improving the security of network components through various standards adoptions is a long-term solution. International information sharing is a shorter-term initiative and one of the most effective ways to increase network security under current conditions.

1.9.1 International cooperative efforts

Sharing information and resources is an important motivation for international cooperation in increasing global security. Nations have already amassed much experience in cooperating to assist in disaster recovery, especially via the International Red Cross, the United Nations, and other formal arrangements. Towards aiding response to a cyber attack, expertise is now developing via information sharing. For example, the G-8[31] Subgroup on High-Tech Crime was formed in January of 1997 and has since been expanded to include a number of non-G-8 countries. This network has been successful in fostering speedy communications between countries to enable preservation of digital evidence for formal legal proceedings.[32]

The G-8 Subgroup, through its meetings with representatives from law enforcement and industry, have developed concrete steps that can be taken to improve cooperation between these two groups and thus allow an expedient and efficient response to incidents. They have developed a checklist of standard procedures for preserving evidence, real-time tracing of communications and user authentication.[33] Such information can assist in locating attackers, halting the advance of an attack and preventing further damage and attack recurrence.

Bilateral cooperation on investigations has been in place for several years and has resulted in successful apprehension of cybercrime perpetrators. The hackers that intruded into more than 500 computer systems in the United States—public (both military and non-military) and private—in early 1998 were identified due to the coordinating efforts of the US National Infrastructure Protection Center (NIPC) and Israeli law enforcement authorities. In 2000, the well-publicized “Denial of Service” (DoS) attacks against Yahoo, Amazon, CNN and others were successfully investigated and the “Mafiaboy” identified due to the cooperative work of the Royal Canadian Mounted Police (RCMP), NIPC and US FBI offices. Also, in 2000, the hackers who stole proprietary information from the Bloomberg financial services company, and then tried to exchange the vulnerability information for ransom, were thwarted through bilateral effort. In that situation, the FBI was able to lure the criminals to London and arrest them with the assistance of Metropolitan Police in London, and law enforcement in Kazakhstan.

Such information and resource sharing has also been directed to promote security education and awareness. The success of the above cases, and many more, has been largely due to trust that has been established over the years by interpersonal relationships between investigators from different countries. The FBI has established “Legal Attaches” (LEGATs) in over 40 countries, providing a liaison to expedite mutual assistance for the United States and the host country. The NIPC has provided cybercrime investigation training to many of its foreign counterparts. Providing training and liaison opportunities are helpful in establishing relationships that offer benefits to network security efforts. Since the founding of NIPC in 1998, Japan, the United Kingdom, Canada, Germany, and Sweden have moved to create agencies with similar functions in their respective countries.

Information and resource sharing can also encourage coordination of legal systems in multiple countries in providing comparable laws that address cybercrime. Further, issues in prevention and prosecution can also be addressed and methods enhanced through collaborative interchange. By sharing experiences, mechanisms can be developed to process investigation-based information, without compromising opportunities for future prosecution. Public accountability can be more assuredly forthcoming, along with access to justice for the victims and those accused of improper use of network systems.

All of the above-mentioned purposes for sharing information have to do with handling security breaches and apprehending and prosecuting criminals. Information sharing also has the potential to increase and escalate

collaborative research, and ultimately to increase the security of application software and the effectiveness of system protection. By far the most valuable purpose for collaboration is to create a more secure network system, one that is increasingly stable, functional, and free of exploitable vulnerabilities.

1.9.2 Clearinghouse initiatives

Many initiatives are already in place to facilitate communication about vulnerabilities in existing hardware and software, known threats in the environment, hacker techniques, and other problems. There is, and needs to be, an enormous amount of data collection, analysis, and diffusion to promote security. However, the volume of information along with the multiplicity of information providers creates difficulties for network operators, who must expend substantial resources to stay up to date with various sources.

System administrators must currently monitor an overwhelming number of sources in order to stay abreast of potential network vulnerabilities.[34] At the same time, system administrators and information security practitioners lack a means for acquiring comprehensive, quantitative statistical data. An information clearinghouse could reduce these shortcomings; international cooperation could ensure that this clearinghouse would be both effective and universally recognized.

A clearinghouse could also serve as an early warning center, notifying system administrators of vulnerabilities and threats as they become apparent. Recognizing the value in this idea, Belgium has advocated a "global early warning system for computer viruses".[35] The United States has just recently announced the Global Early Warning Information System (GEWIS), which is being built by the National Communications System (NCS). This defence agency was established in 1962 so that the US Government can maintain access to adequate communications systems during national emergencies. "The White House believes the monitoring center is necessary because no single entity in the government or private sector has more than a limited view of the global communications network."[36]

In order to gain the benefits of an information clearinghouse, a trust relationship with network users must be established. Business users 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 center 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."[40]

Similar disincentives plagued the maritime shipping industry in the early 1990s as it faced a rising threat from piracy. Shipping companies were reluctant to report incidents of piracy, even though the problem had become quite serious, in fear of damaging their reputations. A regional clearinghouse was created in Kuala Lumpur: the Piracy Reporting Center of the International Maritime Bureau (IMB).[41] The Piracy Reporting Center has been successful as a private organization that collects information from shippers and in turn works with law enforcement agencies to address problems. The IMB Center also performs statistical analyses and uses these data to gain the attention of policy makers in order to convince them to address problems.

The idea of an information clearinghouse is not new: many organizations are currently attempting to fill this role. The Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie Mellon University is a multilateral effort that has served as a central information clearinghouse since its inception in 1988. CERT/CC collects and disseminates information from industry, academic, and government sources. It also has several projects under way for designing tools to enable system administrators to better secure their networks.

Another clearinghouse is industry specific: the Information Sharing and Analysis Centers (ISACs) in the United States. 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 sanitizing and disseminating private sector information to both industry and the NIPC".[42] While valuable, these organizations have membership restrictions and thus limit the speed and breadth of information dissemination—threats to one industry may be applicable to other industries, which might not be warned. As

a result, they do not fulfill the need for a universal agency that collects and disseminates information from all industries and states.

Pottengal Mukundan, of the International Chamber of Commerce (ICC), suggests that his organization is uniquely suited to serve as both an information collection and dissemination center and as an intermediary between the public and private sector. As a non-profit, business oriented association, he believes that the ICC would be readily accepted as a trusted third-party for the receipt of potentially sensitive information. The ICC's policy experience and prior efforts would also enable it to effectively propose policy alternatives to governments. However, its independence might be both a benefit and a concern. To whom would the ICC be responsible and/or accountable?

1.10 Halting cyber attacks in progress

Along with the sharing of information, system administrators also need procedures they can use to assist in ending attacks already under way. This need is particularly evident in DoS attacks, which can be of extended duration and which can shut down business operations while they occur. To aid in ending an attack, system administrators would profit by working with infrastructure operators to trace the attack to its source and then to block the attacker.

Methods for halting attacks in progress as well as those for investigating attacks are constrained by the inability to easily identify and locate attackers. In the case of the Internet, 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. This tracing is a manual process and essentially requires the cooperation of every network operator between the attacker and his target. The inability to automatically trace the source of an attack in real-time significantly impairs the ability of targets and law enforcement agencies to respond to incidents.

One way to automate the identification of attackers would be to change the structure of the Internet by altering the protocols used in packet switching or make changes to the routing system, as examples. Changing the protocols of the Internet has proven difficult, as evidenced by the slow adoption of IPv6.[43] Adding functions to the routers and switches that compose the core of the Internet may be a more viable possibility. Relatively inexpensive additions to hardware and software in current routers could be very helpful in packet tracing.[44]

Automating the tracing of attackers would necessarily reduce the difficulties now required to identify Internet users. Decreasing or eliminating anonymity on the Internet, however, implies significant consequences with respect to Internet culture and use. In particular, the anonymity of the Internet enables free speech for those who might otherwise be persecuted for their beliefs.[45] Such changes therefore should not be made without careful consideration of their consequences.

Any approach to effecting change to packet tracing procedures within the structure of the Internet takes into account the fact that Internet service providers (ISP) and network backbone operators are the most significant agents. 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 challenges of locating attackers by decreasing the number of network operators who must manually search their logs for evidence of the attacker. An organization such as ITU could play a central role in determining the most appropriate solution to this problem and coordinating its acceptance with network operators, especially with telecommunication operators.

1.11 Harmonizing legal systems

"Legal globalism could refer to the spread of legal practices and institutions to a variety of issues, including world trade and the criminalization of war crimes by heads of State."[46] Such legal harmonization can be used to reduce the problems of security in cyberspace. International cooperation would then take place within a shared set of definitions of what constitutes criminal behavior regarding computer networks.

The ability to effectively apprehend and prosecute cyber criminals and terrorists provides a deterrent to cyber attacks. Prosecution of attackers, however, is made extremely difficult by the transnational nature of cyberspace. Imposing criminal liability often necessitates cooperation and coordination between states.

However, many nations have no laws in areas considered important in other nations. Kaspersen and Lodder's[47] international survey of cybercrime documented the incomplete existence of laws for a number of malicious acts, including: unauthorized destruction of data, unauthorized acquisition of data, and unauthorized access to a system. It can be noted that the rapid growth in international networks has not been accompanied by consistent lawmaking in the novel areas of cyber law.[48] Even so, there are initiatives in this area.

The most prominent of these is the Council of Europe Convention on Cybercrime.[49] Although harmonization of laws is just one focus for this treaty, much of the rest of the work depends on this foundation. The Stanford Draft Convention[50] also proposes a legal globalism for cyberspace. Universal participation in this treaty or any other effort that results in the harmonization of laws will help to eliminate "safe havens" for attackers.

Formal agreements seem more likely to encourage universal participation than informal ones. Indeed, formal agreements appear more suitable for a variety of means:

> "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."[51]

An informal effort, with those States that already have cybercrime laws encouraging other States to enact legislation making acts of cybercrime illegal, seems to be a less effective tool but could be a useful interim measure. One potential difficulty is that developing nations may not have the necessary resources to invest in creating this legislation. Efforts such as the ongoing American Bar Association's Cyber Crime Project,[52] however, can provide those nations with a framework of legislation, which they may customize to suit their specific needs.

1.12 Providing assistance to developing nations

Developing nations face particularly severe shortages of resources and trained personnel that both decrease their own security posture and prevent them from effectively providing assistance in such transnational efforts as investigation procedures. Developing nations need an awareness of the problem, as well as laws to address it that are compatible with the needs of the international community; but they also need more. All countries need the capability to assist each other in developing skills in the pursuit of secure networks.

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 different international law enforcement agencies.

> "This training serves not only to make foreign partners more capable of assisting in international investigations and of addressing cybercrime 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."[53]

The NIPC has offered training in classes in the United States, at the International Law Enforcement Academies located in Hungary and Thailand, and in workshops co-sponsored with other nations. Ultimately, though, bilateral efforts are likely to be insufficient for this goal. Many States will need this assistance, and those States able to contribute would undoubtedly prefer not to bear the burden alone.

These efforts need to be expanded to elevate technology resources in all countries. A formal, multilateral effort would help to bring governments and their citizen technologists to a common ground for dealing with security issues.

Finding a suitable framework for international cooperation[54]

1.13 An ideal model

The nature of the problem of infrastructure protection and cyber security, and the sample of partial solutions surveyed in the preceding sections, supports the need for an international framework that might <u>ideally</u> look something like the following. First, each of the governments of the world would have substantial competence to deal with the problem of preventing, thwarting, etc. and punishing attacks on cyber systems. This includes

capabilities and policies in all forms of passive defence to provide effective security for those portions of cyberspace within each government's purview. Second, all connected countries would share a common baseline perception of what constitutes serious (felony) criminal behavior in this new medium. One of the manifestations of this shared perception would be a similar set of laws defining such behavior and offences in each country.[55] Third, each would have substantial capability in active defence, and a competent national authority for engaging in active defence. Finally, international responses to transnational attacks would be covered under a near-universal umbrella convention that would permit timely action, among any combination of countries, under established procedures.

Under these ideal circumstances, we might expect the following standard scenario if a serious cyber attack is launched from Country X against targets in Country A. The victims in A immediately seek help from Government A. Government A determines—perhaps from information shared by Government X—that there is reason to suspect that the attack originated from, or at least passed through, X. Under the umbrella international convention, it immediately contacts the competent authority in X, where the attack is equally viewed as a crime. Government A can count on Government X being willing and able to investigate the extent to which the attack is taking place from X. The competent authority in X will act in a timely manner to help stop the attack if it is still in progress or proceed with other forms of defence. This is essentially the same action that Government A would take if it had the jurisdictional authority to do so itself (albeit subject to such differences in human and civil rights as may exist). Government X may also permit Government A, or an international organization, to participate directly or in an advisory capacity.

Because of all the ideal commonalities under the near-universal arrangement just described, this procedural scenario scales. So, for example, it extends in a straightforward manner if the attack is simultaneously launched from Countries X, Y, and Z against targets in Countries A and B, and the attack is routed through M, N, P and Q.

As far as we can determine, this is the only *unambiguously legal* way to handle active defence on the global scale of the Internet and other large transnational networks. It is also the only way we can conceive of avoiding what is potentially an enormous amount of largely covert actions on the parts of governments against systems and citizens in other countries. It would reduce the errors, collateral damage, and other forms of friction that might arise between nations because of that covert activity.

The present reality is far from this ideal situation. Perhaps most importantly, the great majority of governments of the more than 200 countries with Internet connectivity have little awareness, and less capability, in these areas.

1.14 Necessary characteristics of an approximate real-world construction

So how may we proceed from the current reality to something closer to the ideal international situation? We would argue that we should start to think about the desired structure and content of such an international convention. The timescales associated with conducting and dealing with malicious cyber activities varies from weeks (e.g. the time for new tactical attack modes to emerge) to the comparatively glacial timescales for building extensive and effective international agreements. So, it is necessary to start thinking about the long and iterative process of the latter, even though it is too early to expect solutions to some specific and difficult problems and questions. We might look to a framework that builds in an expectation and means for dealing with the detailed problems of changing technology and standards, over an essentially unbounded time into the future, as well as one intended to help build the capabilities of weaker countries.

What should be included as necessary top-level features in such an international regime? We would suggest the following:

- The focus should be on *serious crimes against computer networks*. The primary concern is protecting the infrastructure, both the IT-based infrastructure itself and the other infrastructures that may be accessed and damaged or manipulated through IT-based control structures. This, we believe, is not the place to address content crimes and issues, such as pornography or intellectual property rights.
- There should be a *harmonization of laws*. Each State party to the convention should adopt a complete set of national laws defining and punishing the full range of serious crimes against computer networks. Although the wording of these laws need not be identical for each country, each

must establish all of the collectively defined malicious behavior specified in the agreement as felonies within the country. Having such a set of laws enacted would be a necessary condition for admission to the convention. We believe that this would also be sufficient for most extradition purposes. What is necessary is to get near congruence of national laws widely accepted and to make the subject a formal, legitimate concern on an extensive international scale.

- There should be a *near-universal set of States parties*.[56] The problem is intrinsically global, and at least some element of a partial solution has to be global. Near-universal participation makes the problem legitimate globally, and tries to eliminate safe havens. Each country connected to the Internet or other global network is part of the threat and vulnerabilities problem, and an effort must be made to try to make each a part of the solution. This is decidedly not the case now.

- A major goal should be to *build international capabilities* to deal with the problem. To this end, we would propose a working organization, perhaps somewhat similar to the International Civil Aviation Organization (ICAO) that exists for the aviation transportation infrastructure.[57] This organization would help to develop standards, best practices, and provide training and technology on a global scale, and especially for the large number of countries that have little or no capacity to do everything for themselves in the cyber domain at this time. This applies to both passive and active means of defence. Another organization that could serve as a partial model in this context may be the Internet Engineering Task Force (IETF), a volunteer and very public organization that is essentially the custodian and modifier of basic Internet protocols. We tentatively dub this new organization the Agency for Information Infrastructure Protection (AIIP).

- *Avoid building too much technical or procedural detail into the basic agreement*. At this time, nobody understands the technological and procedural means or costs well enough to appreciate what it would take to require them on a large scale. It will take some time for thoughts and technology to mature to the point where such might be recommended or required. We recommend setting up a forum and means, e.g. through the AIIP, for the necessary discussions and work to take place. As is the case in other international domains, industry and academic participation in these efforts would be essential.

- The prospective convention is *not meant to apply to the actions of States*. We assume that there are dozens of nation States investigating the possibilities of so-called information warfare or information operations. Few of those would presumably be interested in constraining themselves at this early stage. This is not meant to be an arms control convention, just as the various widely accepted agreements on safety and security in civil aviation (among other areas) are not meant to apply to the air forces of the nation States of the world with regard to their national security activities.

- For the purposes of a formal multilateral treaty, we take the view that it is both *difficult and unnecessary to precisely define "cyberterrorism."* There is unlikely to be much agreement among a wide spectrum of interested parties on such a definition given the enormous variety of malicious activity possible in this medium, and the range of motivations behind the spectrum of possible attacks. It is difficult to distinguish an early stage of an attack as either crime or terrorism, and even the final determination may depend on the "eyes of the beholder." We take the approach of defining serious forms of crimes against information systems under the assumption that essentially all forms of what would widely be considered cyberterrorism would be egregious instances of these crimes. Furthermore, we add to the list of serious offenses "the uses of a cyber system as a material factor in committing an act made unlawful or prohibited" by a number of widely adopted international conventions intended to deal with terrorism, e.g. The International Maritime Organization Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation [Maritime Terrorism Convention] of March 10, 1988.[58] As in other contexts, e.g. safety and security in civil aviation, the nature of the attack is what matters; the motivation of the attacker should not be a determining factor.

- States parties would *not violate the civil or human rights* of their citizens. No State party would be expected to compromise its own laws in this regard. So, for example, assume that both the United States and Iran are signatories. Say that an American citizen is suspected of attacking an Iranian system in a manner that is against the laws that both countries have agreed upon as part of signing the convention. If the United States suspects that this person's human rights would be at risk if

extradited to Iran, then the United States is obligated to try that person on its territory for that crime. Another alternative is to extradite him for trial to a third country that has a claim to jurisdiction but observes civil or human rights laws similar to those in the United States. In this regard, we observe that a harmonization of laws in the form of defining felonies does not also necessarily imply a harmonization of investigative law or procedures. Although some progress may be made to harmonize laws and procedures that pertain to privacy, seizure of assets, permitted incarceration periods without charge, etc. significant differences among countries will remain.

1.15 International cooperation initiatives

1.15.1 Cyberspace initiatives

A group at Stanford University framed a draft convention, first mentioned in Section 3.4, based on these requirements.[59] Others, including the Secretary-General of ITU, have brought up the issue of an extensive international agreement on security.[60] A treaty that has been taken farthest towards implementation is the Council of Europe's *Convention on Cybercrime*.[61] Twenty-six members and four non-members signed the COE Convention on 23 November 2001.[62] As of February 2003, only two have ratified it.

The COE Convention is geared towards law enforcement. It addresses a wide range of crimes against computer networks, but also includes computer-related offences (forgery and fraud) and crimes of content covering child pornography and intellectual property. All signatory countries are required to have a harmonized set of laws in accordance with those listed in the Convention. It may ultimately aspire to near-universality, but the focus so far has been on Europe and some advanced outside countries. It is not explicitly concerned with capacity building. A large part of the agreement is concerned with procedural law, with extensive requirements on the collection, storage, etc. of information that may prove to be relevant in criminal cases, and with strong requirements on private service providers. International cooperation is much concerned with extradition, mutual assistance procedures, information sharing, capture, and preservation largely for the purposes of criminal investigation.[63] There are concerns and reservations with regard to civil rights. If one assumes that full capabilities as required by the Convention are a prerequisite for membership, then this convention arguably has a very high barrier to entry for a great many countries.

1.15.2 Initiatives in other domains

We also note that reasonably effective agreements exist in other domains along the lines enumerated after the bullets in Section 4.2. Perhaps the closest analogy is with civil aviation, which itself also happens to be extensively and increasingly dependent on cyber systems.[64] There are others covering intrinsically transnational domains such as maritime transportation and piracy, health, and pollution.

1.15.3 Problems with cooperation initiatives for cyberspace

We are a long way from having such an agreement for actions in cyberspace, and there will be considerable difficulties along any path to an effective approximation. We touch on a few of the problems below.

- As with many international agreements, questions arise as to forms of enforcement and sanctions against signatories who are not meeting the conditions or who are in conscious violation.
- Work needs to be done on estimating the costs of such a convention. Just two examples of such costs include an estimate of the volume and prospective growth rates of requests and investigations that would need to be handled, and the cost of setting up and running an organization like the AIIP, and the competent national authorities. In terms of savings, we note that major cyber attacks (e.g. via virus or denial of service) have been estimated to cost hundreds of millions of dollars. So, as in the case with averted airline disasters, every prevented major incident represents huge "savings."
- As noted earlier, much of active defence is intelligence intensive. How will information and evidence be effectively shared among a diverse set of affected parties without compromising national interests?
- Private organizations, e.g. commercial Internet service providers (ISP), are key players in the global information infrastructures. Their cooperation and technology would be crucial to the effectiveness of any international regime to protect and assure those infrastructures. Many are extensively multinational in their operations. Who would they have to respond to? Where do their

responsibilities and liabilities lie if there are many competing governments with different laws, e.g. on privacy, requests data, and other forms of cooperation?

- How do we effectively scale up to a near universal sign-up? In addition to the obvious approach of simply starting with a small number of countries, possibilities include the use of more limited agreements as "building blocks" to acquire subsets of partners and experience with "what works." These more limited agreements might be done multilaterally, based on sector (e.g. for the cyber dimensions of civil aviation) or regional (e.g. for Europe) domains.
- A related question is what to require of a State party as a condition for admission? Two possibilities are a set of harmonized domestic laws and the existence of a designated competent authority. Another related issue is what to do with the non-signatories? For example, should (or could) an effort be made to create a form of network quarantine?

Because of the law enforcement nature of important parts of any such convention, we would expect that it would have to be under an umbrella that would be widely recognized by governments, e.g. under ITU or COE.

We note that neither the COE nor the Stanford Draft conventions have yet very good solutions to these problems. In particular, the COE appears to be giving priority to signing up as many countries as possible with no strong entry requirements as to capabilities, or clear specifications as to how these capabilities are to be met over time. In this regard, as of February 2003, we note that Albania is one of only two countries to actually ratify the convention.

1.15.4 Problems in a partially private approach?

The "normal" model for international cooperation as described above would have the AIIP as a derivative of the convention, i.e. as a body "enabled" by the convention much as the ICAO is enabled by the international conventions for civil aviation. But broad-based multilateral conventions are very hard to establish, and often take a long time. One way of dealing with several of the problems noted above may be to "put the cart before the horse" by establishing an AIIP along the lines of the IETF or the Computer Emergency Response Teams (CERT) models before the international convention is established.[65]

A private version of the AIIP might initially establish itself as a useful and respected organization, provide a vehicle for working with the private sector in this subject area, and form a nucleus around which the signatory nations could "condense" as the international convention develops.[66] Initial funding would not have to come from some sort of tortuous process of securing funding from multiple governments to set up another diplomatically crafted Geneva-based agency. It could be established by industry or by limited and essentially detached US Government funds, as was the case with what was essentially the early IETF predecessor or CERT, or by detached funding from a small number of governments or foundations, with the intent of having it taken under the international convention in time.

However, a private entity would have to be careful not to encroach on the powers of national governments and, thus, would not be able to realize all of the functions discussed earlier. The power to make laws, to investigate suspicious acts, and to punish criminals lies with governments. No one contemplates locating police powers in a private entity for instance, for it would lack a basis in legitimacy to exercise such powers.

Nonetheless, a private entity could play a supporting role to sovereign states. Governments that have not formally joined an international regime but that support security cooperation might be willing to work with a private global entity, realizing the benefits of cooperation while avoiding the politically significant act of making binding agreements with other governments.

Of the forms of international cooperation identified earlier, a number could be facilitated by a private entity through information sharing. To promote the diffusion of security standards, a private entity could gather, analyze, and diffuse information about such standards. Information about available technology, as well as regulatory-, procurement-, and liability-based strategies for implementation could be shared. Legal harmonization could be facilitated in a similar manner. A private entity could identify emerging regulatory practices that have worked well in some countries and publicize them in other countries. Or it could draft and diffuse model legislation appropriate for many different countries. Assistance to developing nations might also be delivered through such an entity, either as information sharing or through active training

programmes. This is essentially what Pottengal Mukundan of the International Chamber of Commerce (ICC), discussed in Section 3.2.2, has suggested.

While a model incorporating a private sector group may have merit, experiences caution that it may have difficulties. The Internet Corporation for Assigned Names and Numbers (ICANN), created in 1998 to manage domain names and Internet protocol numbers, encountered issues as a private entity drifting into substantive policy-making.[67] In making rules about the availability and acceptable content of domain names, ICANN began to encroach on the policy-making prerogatives of governments. ICANN's rules for the creation of new top-level domain names (e.g. *.biz*) constituted a competition policy for the domain name market, while its rules for defining trademarks in domain names broke new ground in global intellectual property rights. The organization became the target of severe criticism from industry, civil society groups, and governments alike.

Taken to the extreme, privatization of coordination can open the door to a policy process lacking transparency and accountability, subject to mission creep, and vulnerable to special interest capture. Such deficiencies would be especially problematic for an organization whose main task is security, and whose activities would be weighted towards active defence. This last requirement would ultimately necessitate a framework with government as the primary unit of participation.

In summary, private approaches to global security offer benefits, but they have to observe strict limits. An extensive private programme of information sharing could promote intergovernmental coordination. However, should a non-governmental entity begin to exercise governmental powers, e.g. developing the ability to trace packets, it might quickly find itself subject to criticism.

Concluding remarks

The security issues in our networked systems as described in this paper identify some of the work that needs to be done, and the urgency with which concerns need to be addressed. Dependence on some of the IT-based infrastructures in several countries is such that serious national consequences could result from the exploitation of their vulnerabilities. And as the density of networks increases, the necessity for transnational participation in improving network security increases.

The changing technologies and the potential for changing threats is taxing our understanding of the threats and how to deal with them. When we approach the notion of "visions" of an information society, there are problems with describing this society as utopian in character. Globalism complicates the dilemma. As described by Keohane and Nye[68], the interdependence of nations in complicity must now be considered multiple relationships, not simply single linkages, and as multi-continental distances, not simply regional networks.

Due to the complexity and entanglement among networks and communities internationally, any increases in network security must involve the concerted efforts of as many nations as possible. We have ample experience in international regimes to understand that a great deal can be accomplished through such mechanisms, but not without taking note of their earlier trouble spots.

We must learn from prior unexpected consequences in international cooperation, just as in the battle to secure networked systems, and be ever more cautious as we move forward toward some type of international action. But move forward quickly we must if the benefits from the use of our networked systems are to be realized in the myriad ways that they have been and are hoped for in the future. Nations must cooperate fully within their capability in order to contain the actions of those who threaten our networks, and to realize the positive vision that we have for our societies.

References

American Bar Association. International Cyber Crime Project of the ABA Privacy and Computer Crime Committee : http://www.abanet.org/scitech/computercrime/cybercrimeproject.html.

Batista, E., IDC: Tech Bucks, Hack Threats Up, Wired News, 23 December 2002: http://www.wired.com/news/infostructure/0,1377,56902,00.html.

Brush, C., Surcharge for Insecurity. Information Security Magazine, July 2001: http://www.infosecuritymag.com/articles/july01/departments_news.shtml.

CERT/CC, CERT/CC Statistics 1988-2002, 5 April 2002: http://www.cert.org/stats/cert_stats.html.

Coglianese, C., Globalization and the Design of International Institutions, In J. S. J. Nye, and John D. Donahue (Ed.), Governance in a Globalizing World, Washington D.C., Brookings Institution Press, 2002.

Conry-Murray, A.Kerberos, Computer Security's Hellhound, Network Magazine, 5 July 2002, http://www.commweb.com/article/NMG20010620S0008/1.

Council of Europe, Convention on Cyber crime ETS no.: 185 - Explanatory Report (Article II, Section II) 23 November 2001: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

Fisher, D., Open Source: A False Sense of Security, eWeek, 30 September 2002: http://www.eweek.com/print_article/0,3668,a=31672,00.asp .

Gates, B., Trustworthy Computing, Wired News, 17 January 2002: http://www.wired.com/news/business/0,1367,49826,00.html.

Goodman, M. D., and Brenner, Susan W. The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, 2002: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php.

Goodman, S. E., Toward a Treaty-Based International Regime on Cyber Crime and Terrorism, in J. Lewis (Ed.), Transnational Cyber Security Cooperation: Challenges and Solutions, Washington, DC, 2002,: CSIS Press.

Goodman, S. E., M. Cuellar, and H. Whiteman, Chapter 3: Civil Aviation. In A. D. Sofaer, and Seymour E. Goodman (Ed.), The Transnational Dimensions of Cyber Crime and Terrorism. Stanford, CA: Hoover Institution Press, 2001.

Goodman, S. E., Pamela B. Hassebroek, Davis King, and Andy Ozment, 20-22 May 2002, International Coordination to Increase the Security of Critical Network Infrastructures. International Telecommunication Union: http://www.itu.int/osg/spu/ni/security/docs/cni.04.pdf.

Harris, S., The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force, RFC 3160, Internet Engineering Task Force, August, 2001: http://www.ietf.org/tao.html.

Hudson, H. E., Global Connections: International Telecommunications Infrastructure and Policy, New York: John Wiley & Sons, Inc., 1997.

International Telecommunication Union (ITU), Creating Trust In Critical Network Infrastructures, 2002: http://www.itu.int/osg/spu/ni/security/index.html.

International Telecommunication Union (ITU), Report of IP-Telecoms Interworking Workshop, ITU, Geneva, 25-27 January 2000, http://www.itu.int/ITU-T/worksem/ip-telecoms/index.html.

Japan Country Report, Transnational Cyber Security Cooperation: Challenges and Solutions, 2002, Washington D.C.: CSIS Press, (Forthcoming).

Ji-young, S., Civic Group Considers Pressing Charges Against Microsoft for Internet Crash, The Korea Times, 3 February 2003: http://times.hankooki.com/lpage/nation/200302/kt2003020318021611960.htm.

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

Sofaer, A. D., Responding to Transnational Cyber Crime, Washington D.C., 2001: Workshop on Protecting Cyberspace: The International Dimension, The Georgia Tech Information Security Center (Georgia Institute of Technology) and the Center for International Security and Cooperation (Stanford University).

Sofaer, A. D., and Seymour E. Goodman, A Proposal for an International Convention on Cyber Crime and Terrorism, 2002, Stanford, CA: Center for International Security and Cooperation, Stanford University.

Sofaer, A. D., and Seymour E. Goodman (Ed.), The Transnational Dimension of Cyber Crime and Terrorism, 2001, Stanford, CA: Hoover Institution Press.

Sofaer, A. D., Gregory D. Grove, and George D. Wilson, Draft International Convention to Enhance Protection from Cyber Crime and Terrorism, in Abraham D. Sofaer, and Seymour E. Goodman (Ed.), The Transnational Dimension of Cyber Crimes and Terrorism, 2002: The Hoover Institution on War, Revolution and Peace.

Soo Hoo, Kevin, Seymour Goodman, and Lawrence Greenberg, Information Technology and the Terrorist Threat. Survival, International Institute for Strategic Studies, London, 1997, 39(3), 135-155.

Vatis, M., International Cyber Security Cooperation: Informal Bilateral Models, Transnational Cyber Security Cooperation: Challenges and Solutions (Forthcoming ed.). Washington D.C., 2002: CSIS Press.

Wenger, A., Jan Metzger and Myriam Dunn (Ed.), CIIP Handbook: An Inventory of Protection Policies in Eight Countries, 2002, Zurich: Center for Security Studies and Conflict Research.

Wheeler, D. A., Secure Programming for Linux and Unix HOWTO, 3 March 2003: http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO/index.html.

Wilson, J. S., The New Trade Agenda: Technology, Standards, and Technical Barriers. SAIS Review, 16(1), 1996, 67-91.

Wolcott, P., and Seymour E. Goodman, The Internet in Turkey and Pakistan: A Comparative Analysis, 2000, Stanford, CA: Stanford University Institute for International Studies, Center for International Security and Cooperation.

[1] For example, Hong Kong, China, is such an entity that retains its own top-level domain name.

[2] See Peter Wolcott and Seymour E. Goodman, The Internet in Turkey and Pakistan: A Comparative Analysis, 2000: Center for International Security and Cooperation, Stanford University. Studies of the diffusion and absorption of the Internet in various parts of the world are also increasingly available.

[3] "Assurance" means that a system does what it is supposed to do, and does not do anything else. Security is protection against hostile actions. The two overlap but are not identical. However, for convenience our use of the term "security" is usually meant to include the concept of assurance. For definitions and illustrations of many other terms, see Bruce Schneier, Secrets and Lies, Digital Security in a Networked World, John Wiley, New York, 2000. "Trust" is a term that has been used more or less synonymously with "assurance", e.g. National Research Council, Trust in Cyberspace, National Academy Press, Washington DC, 1999.

[4] On 22 October 2002, a DoS attack against 13 "root servers" that provide the primary interconnection for almost all Internet communications suggests the potential for future attack. See E. Batista, IDC: Tech Bucks, Hack Threats Up, 23 December 2002, Wired News: http://www.wired.com/news/infostructure/0,1377,56902,00.html.

[5] Kevin Soo Hoo, Seymour Goodman, Lawrence Greenberg, Information Technology and the Terrorist Threat, Survival, International Institute for Strategic Studies, London, 39(3), 1997, 135-155.

[6] Most of this section is taken and edited, with permission, from Stephen Lukasik, Seymour Goodman, David Longhurst, Strategies for Protecting National Infrastructures Against Cyber Attack, 2003, International Institute for Strategic Studies, London. This Adelphi Paper discusses strategic options, required capabilities, and responsible parties in greater detail than is possible here.

[7] Schneier, 2000.

[8] Stephen J. Lukasik, Public and Private Roles in the Protection of Critical Information-Dependent Infrastructure, Center for International Security and Cooperation, Stanford University, 1997.

[9] Information in this section has been previously discussed as "Opportunities for Action" in S.E. Goodman, Pamela B. Hassebroek, Davis King, and Andy Ozment, International Coordination to Increase the Security of Critical Network Infrastructures, International Telecommunication Union, 20-22 May 2002: http://www.itu.int/osg/ni/security/docs/cni.04.pdf.

[10] "Malicious software includes viruses, Trojan horses, and worms. Together these are called *malware*." Schneier, p. 151.

[11] Susan Harris, ed, The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force, Internet Engineering Task Force RFC 3160, August 2001: http://www.ietf.org/tao.html.

[12] International Telecommunication Union, Report of IP-Telecoms Interworking Workshop,, ITU, Geneva, 27 January 2000: http://www.itu.int/ITU-T/worksem/ip-telecoms/index.html.

[13] Bill Gates, Trustworthy Computing, [Online], Wired News, 17 January 2002: http://www.wired.com/news/business/0,1367,49826,00.html.

[14] David A. Wheeler, Secure Programming for Linux and Unix HOWTO, 3 March 2003: http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO/index.html.

[15] According to Emily Frye, Associate Director of Legal Programs at the Critical Infrastructure Protection Project, the largest US-based testing and screening body is The Debian Project, which was begun in 1993 and distributes the Debian Linux open-source software. See also the Open Source Initiative, 14 April 2003: http://www.opensource.org/index.php.

[16] Dennis Fisher, Open Source: A False Sense of Security, eWeek, 30 September 2002: http://www.eweek.com/print_article/0,3668,a=31672,00.asp.

[17] Fisher, 2002.

[18] Alex Salkever, Open-Source Security Is Opening Eyes,, BusinessWeek Online, 19 November 2002: http://www.businessweek.com/technology/content/nov2002/tc20021119_3974.htm.

[19] Emily Frye, private communication 10 April 2003.

[20] Andrew Conry-Murray, Kerberos: Computer Security's Hellhound, Network Magazine, 5 July 2001: http://www.commweb.com/article/NMG20010620S0008/1.

[21] OECD, Guidelines for the Security of Information Systems, Organization for Economic Cooperation and Development, 25 July 2002: http://www.oecd.org/pdf/M00034000/M00034292.pdf.

[22] OECD,, Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, Organization for Economic Cooperation and Development, 21 January 2003: http://www.olis.oecd.org/olis/2002doc.nsf/LinkTo/dsti-iccp-reg(2002)6-final.

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

[24] Japan Country Report, 2002, in Transnational Cyber Security Cooperation: Challenges and Solutions, Washington, DC: CSIS Press, (forthcoming).

[25] Colleen Brush, Surcharge for Insecurity, Information Security Magazine, July 2001: http://www.infosecuritymag.com/articles/july01/departments_news.shtml.

[26] Ira Sager, and Jay Greene, The Best Way To Make Software Secure: Liability, 18 March 2002, Business Week, 61.

[27] People's Solidarity for Participatory Democracy (PSPD) said it is considering filing a class action suit against the software giant for the "Slammer" worm that paralysed Korea's Internet servers on 25 January by unleashing huge volumes of Internet traffic. The worm was traced to a widely known flaw in Microsoft's SQL software, a web server application. See: Ji-young, S.,, Civic Group Considers Pressing Charges Against Microsoft for Internet Crash, The Korea Times., 3 February 2003: http://times.hankooki.com/lpage/nation/200302/kt2003020318021611960.htm.

[28] Cary Coglianese, Globalization and the Design of International Institutions, in J. S. Nye, and John D. Donahue (Ed.), Governance in a Globalizing World. Washington, D.C., 2000: Brookings Institution Press, 299.

[29] H. E. Hudson,, Global Connections: International Telecommunications Infrastructure and Policy, 1997, New York: John Wiley & Sons, Inc., 397.

[30] J. S. Wilson, The New Trade Agenda: Technology, Standards, and Technical Barriers, 1996, SAIS Review, 16(1), 67-91.

[31] The members of the Group of Seven (G-7) are Canada, France, Germany, Italy, Japan, the United Kingdom and the United States. The leaders of these largest industrialized democracies have met annually since 1975 to discuss economic and political issues. The Group of Eight (G-8) is made up of the G-7 nations plus the Russian Federation, which officially became the eighth member in 1997.

[32] M. Vatis, International Cyber Security Cooperation: Informal Bilateral Models, 2002, Transnational Cyber Security Cooperation: Challenges and Solutions, Washington, DC: CSIS Press, Forthcoming.

[33] Vatis, (2002).

[34] Frequently used sources include the Bugtraq mailing list, CERT/CC, CIAC, vendor specific mailing lists, SANS, SecurityTracker.com, and many other websites and mailing lists.

[35] P. Mukundan, 2002, Laying the Foundations for a Cyber-Secure World, In Transnational Cyber Security Cooperation, Challenges and Solutions, Washington, DC, CSIS Press, Forthcoming.

[36] Brian Krebs, Feds Building Internet Monitoring Center, , Washington Post, 31 January 2003: http://www.washingtonpost.com/ac2/wp-dyn/A3409.

[37] Frequently used sources include the Bugtraq mailing list, CERT/CC, CIAC, vendor specific mailing lists, SANS, SecurityTracker.com, and many other websites and mailing lists.

[38] P. Mukundan, 2002, Laying the Foundations for a Cyber-Secure World, In Transnational Cyber Security Cooperation: Challenges and Solutions, Washington, DC: CSIS Press, Forthcoming.

[39] Brian Krebs, Feds Building Internet Monitoring Center, Washington Post, 31 January 2003: http://www.washingtonpost.com/ac2/wp-dyn/A3409-2003Jan30.

[40] Mukundan, 2002.

[41] Mukundan, 2002.

[42] See: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, 1998, http://www.nipc.gov/about/pdd63.htm.

[43] Systems on the Internet use the Internet Protocol (IP) to communicate. Version six of that protocol (IPv6) is designed to replace version four, the current standard.

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

[45] L. Lessig, (1999), Code and Other Laws of Cyberspace. New York: Basic Books.

[46] R. O. Keohane, and Joseph S. Nye, Jr. (2000), Introduction, In J. Joseph S. Nye, and John D. Donahue (Ed.), Governance in a Globalizing World: Brookings Institution Press.

[47] H. W. K. Kaspersen, and A.R. Lodder, (2000, April 15), Overview of the Criminal Legislation Addressing the Phenomenon of Computer-Related Crime in the United Nations Member States, [Online], United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (UNAFEI) Report, Available: http://www.rechten.vu.nl/~lodder/papers/unafei.html [2003, January].

[48] M. D. Goodman, and Susan W. Brenner, (2002), The Emerging Consensus on Criminal Conduct in Cyberspace, [Online], UCLA Journal of Law and Technology, Available: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php [2002, January].

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

[50] Abraham D. Sofaer et al., (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.

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

[52] American Bar Association, International Cyber crime Project of the ABA Privacy and Computer Crime Committee, [Online] Available: http://www.abanet.org/scitech/computercrime/cybercrimeproject.html [2003, February].

[53] Vatis, (2002). Much of the other information in this paragraph was also taken from this source.

[54] Although expanded and edited, this section has been taken directly, with permission, from Seymour E. Goodman, (2002), Toward a Treaty-Based International Regime on Cyber Crime and Terrorism, In J. Lewis (Ed.), Transnational Cyber Security Cooperation: Challenges and Solutions. Washington, DC: CSIS Press, Forthcoming.

[55] The project of the American Bar Association is attempting to assemble a survey of and guide to world cyber laws. American Bar Assn., (2003). Another set may be found in the COE Convention: Council of Europe, Convention on Cyber Crime, European Treaty Series – No. 185, Budapest, 23.XI.2001. Another more extensive survey may be found in Goodman and Brenner, (2002).

[56] An approach built on a large set of bilateral, trilateral, etc. agreements to achieve what was outlined under the "ideal" agreement earlier would be combinatorially explosive for over 200 countries. See Goodman, (2002), for some basic calculations.

[57] See S.E. Goodman, M. Cuellar, and H. Whiteman, (2001). Chapter 3: Civil Aviation, In Abraham D. Sofaer, and Seymour E. Goodman (Ed.), The Transnational Dimensions of Cyber Crime and Terrorism, Stanford, CA: Hoover Institution Press. On the surface the case of civil aviation would seem to be simpler, at least partly because its defence is more discrete in that there is a much smaller number of targets (aircraft and airports), and these are physically easy to locate. It should also be noted that civil aviation is heavily dependent on information systems for many functions.

[58] An explicit and extensive list of these conventions is provided in Article 3, Paragraph 1(f) of the Stanford Draft.

[59] Abraham D. Sofaer, Seymour E. Goodman, et al., A Proposal for an International Convention on Cyber Crime and Terrorism, Center for International Security and Cooperation, Stanford University, August 2000. Article 1, Paragraph 2, which unnecessarily attempts to define "cyberterrorism," should be considered deleted. Hereafter this draft convention will be referred to as the Stanford Draft. More general and extensive coverage of the international aspects of cybercrime and law may be found in Abraham D. Sofaer and Seymour E. Goodman, Eds. The Transnational Dimensions of Cyber Crime and Terrorism. Hoover Institution Press, Stanford University, Stanford, CA. 2001. The AIIP is first defined in the Stanford Draft. For some further discussion on its functions, make-up, etc., see S. J. Lukasik, What Does an 'AIIP' Do? Presentation notes, Georgia Institute of Technology, Atlanta GA, May 27, 2000.

[60] Martyn Williams, (2003, January 13), UN Summit could spark Net regulation talks, [Online], IDG News Service, Available: http://www.infoworld.com/article/03/01/13/030113hnwsis_1.html [2003, February].

[61] Council of Europe. (2001, November). Convention on Cyber crime ETS no.: 185 - Explanatory Report (Article II, Section II), [Online]. Available: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm [2003, January].

[62] Brian Krebs, (2001, November 26). Thirty Nations Sign Cybercrime Treaty. Newsbytes. Available: http://online.securityfocus.com/news/291 [2003, February].

[63] For a critique of Draft 25 of the COE Convention, see Abraham D. Sofaer, (2001), Responding to Transnational Cyber Crime, Washington D.C.: Workshop on Protecting Cyberspace: The International Dimension, The Georgia Tech Information Security Center (Georgia Institute of Technology) and the Center for International Security and Cooperation (Stanford University). A copy of this paper may be obtained from the present authors.

[64] See S. Goodman, M. Cuellar, and H. Whiteman, (2001), footnote 50 above.

[65] Stephen J. Lukasik, private communication June 28, 2001, suggested this inverted approach.

[66] While this paper is devoted primarily to government coordination, private groups play a role at many levels. There is indeed a significant role for private organizations in enabling increased network security, but extensive discussion of possible formal cooperation in the private sector is beyond the scope of this paper.

[67] For more detailed discussions of ICANN and its problems, see Hans Klein, (2002), ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy, The Information Society, 18:193-207, 2002; and Milton Mueller, (2002), Ruling the Root. Cambridge, MA: MIT Press.

[68] Keohane and Nye, (2000).