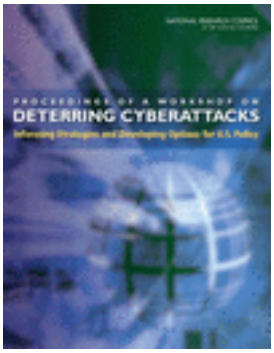

Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy

Committee on Deterring Cyberattacks: Informing Strategies and Developing Options; National Research Council

ISBN: 0-309-16086-3, 400 pages, 8 1/2 x 11, (2010)

Cyber Security and International Agreements

Abraham D. Sofaer
Hoover Institution

David Clark
Massachusetts Institute of Technology

Whitfield Diffie
Internet Corporation for Assigned Names and Numbers

Society has become dependent on cyber systems across the full range of human activities, including commerce, finance, health care, energy, entertainment, communications, and national defense. "The globally-interconnected digital information and communications infrastructure known as 'cyberspace' underpins almost every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, public safety, and national security."[1] The U.S. is especially vulnerable to cyber insecurity because it depends on cyber systems more heavily than most other states. But cyber insecurity is a worldwide problem, potentially affecting all cyber systems and their dependent infrastructure.

Cyber insecurity can result from the vulnerabilities of cyber systems, including flaws or weaknesses in both hardware and software, and from the conduct of states, groups, and individuals with access to them. It takes the forms of cyber warfare, espionage, crime, attacks on cyber infrastructure, and exploitation of cyber systems.

Virtually all aspects of cyber insecurity have a transnational component, affecting users of cyber systems throughout the world. Nonetheless, current U.S. efforts to deter cyberattacks and exploitation—though formally advocating international cooperation—are based almost exclusively on unilateral measures.[2] Whether cyberdeterrence through these methods can provide an adequate level of cyber security for U.S. users is, in the view of the NRC Committee on Deterring Cyberattacks (hereinafter "Committee"), an open question. Proposals for the U.S. to consider additional, unilateral measures to deter cyberattacks through prevention and retaliation have been presented to the NRC Committee for

NOTE: This paper has benefited from valuable comments made by members of the NRC Committee on Deterring Cyberattacks, for which the authors are grateful. We also thank Seymour Goodman for his support, as well as Leisel Bogan, Courtney Matteson and Thomas Church for their invaluable research assistance.

[1]The White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," May 2009, p. iii.

[2]A recent example is the comprehensive and influential "Securing Cyberspace for the 44th Presidency," A Report of the CSIS Commission on Cybersecurity for the 44th Presidency (Washington, D.C. 2008), which contains numerous, sweeping recommendations to restructure government agencies and adopt national programs to secure various aspects of the U.S. cyber infrastructure, while proposing virtually no program of international engagement. This follows from the Report's premise that the activities of foreign states are the source of cyber insecurity in the U.S. (p. 11): "Foreign opponents, through a combination of skill, luck, and perseverance, have been able to penetrate poorly protected U.S. computer networks and collect immense quantities of valuable information."

its consideration. But, as the Committee has noted, measures associated with classical deterrence are difficult to employ against cyberattacks and exploitation.[3] States, groups, and even individuals can easily launch attacks upon or attempt to exploit cyber systems. The sources of attacks and exploitations are difficult to determine within time frames that enable victims to avoid damage, and any defensive measure is likely eventually to fail given the vulnerabilities of most cyber systems and the incapacities of users.

These considerations led the NRC Committee to conclude that, "whatever the useful scope for deterrence, there may also be a complementary and helpful role for international legal regimes and codes of behavior designed to reduce the likelihood of highly destructive cyberattacks and to minimize the realized consequences if cyberattacks do occur. That is, participation in international agreements may be an important aspect of U.S. policy."[4] Various forms of international cooperation do currently exist, and international agencies and private entities play or are attempting to secure significant roles in cyber security. For over a decade, however, the U.S. government—while complaining about cyberattacks, espionage, and exploitation by other states and non-state actors—has avoided international arrangements that go significantly beyond obligating a group of predominantly European states to criminalize and cooperate in prosecuting specified forms of conduct. This policy is, appropriately, changing. Both the Executive branch and Congress are now considering ways in which international cooperation and agreements could enhance cyber security.

The potential utility of international cybersecurity agreements deserves to be carefully examined. International agreements covering other transnational activities, including armed conflict, communications, air and sea transportation, health, agriculture, and commerce, among other areas, have been widely adopted by states to enhance safety and efficiency through processes that could well be useful in regulating cyber activities.

Transnational agreements that contribute to cybersecurity will only be possible, however, if they take into account the substantial differences that exist between activities regulated by established international regimes and cyber systems. Many states will be unprepared at this time to agree to limit their control of cyber activities they regard as essential to their national security interests. International agreements will also be impossible where irreconcilable differences in policies exist among states, particularly regarding political uses of the Internet, privacy, and human rights. But, while these factors limit the potential scope and utility of international cyber-security agreements, they do allow for international cooperation on many issues that could prove beneficial.

The potential for improving cyber security through international agreements can best be realized through a program that identifies: the activities likely to be subjects of such agreements and those that are not; the measures likely to be used by parties to improve cyber security in each area of activity appropriate for international cooperation; and the form which any international body that may be utilized or established for this purpose should assume, the authority such a body would be assigned, and the basis upon which its activities would be governed. International agreements negotiated on the basis of these practical premises could help to create a more secure cyber environment through measures that go beyond conventional forms of deterrence.

I. THREATS TO CYBER SECURITY

Retired Admiral Dennis Blair, former U.S. Director of National Intelligence, testified in early 2010 that increasingly sophisticated enemies "severely" threaten some U.S. information systems: "Sensitive

[3]See Chapter 9, National Research Council (NRC), *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, ed. William Owens, Kenneth Dam, and Herbert Lin (Washington D.C.: The National Academies Press, Washington, D.C., 2009). See also Section 2.2, (NRC) "Letter Report from the Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy" March 25, 2010, p. 6.

[4]Letter Report from the Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, National Research Council, March 25, 2010, p. 19.

information is stolen daily from both government and private sector networks, undermining confidence in our information systems, and in the very information these systems were intended to convey. . . . Malicious cyber activity is occurring on an unprecedented scale with extraordinary sophistication."[5] Former Vice-Admiral Mike McConnell, Blair's predecessor and head of the National Security Agency ("NSA") from 1992 to 1996, wrote recently: "The United States is fighting a cyber-war today, and we are losing. It's that simple. As the most wired nation on Earth, we offer the most targets of significance, yet our cyber-defenses are woefully lacking."[6] Howard Schmidt, White House Cyber Security advisor, agrees that cyber threats exist, but denies we are in a "war"; others similarly criticize such statements as exaggeration.[7] It is widely agreed, however, that various vulnerabilities and forms of hostility have exposed cyber systems, including the Internet, to attack and infiltration, inflicting substantial costs in the form of financial losses and defensive measures and creating even more substantial, future dangers to the nation's critical infrastructures.[8] President Obama's 2009 Cyberspace Policy Review concludes: "a growing array of state and non-state actors such as terrorists and international criminal groups are targeting U.S. citizens, commerce, critical infrastructure, and government. These actors have the ability to compromise, steal, change, or completely destroy information."[9]

Cyber insecurity stems from the fact that cyber systems have been designed to facilitate access and utilization, rather than security. "The architecture of the nation's digital infrastructure, based largely upon the Internet, is not secure or resilient. Without major advances in the security of these systems to make them sufficiently secure or resilient, it is doubtful that the United States can protect itself from the growing threat of cybercrime and state-sponsored intrusions and operations."[10]

Threats to cyber security can be roughly divided into two general categories: actions aimed at and intended to damage or destroy cyber systems ("cyberattacks"), and actions that seek to exploit the cyber infrastructure for unlawful or harmful purposes without damaging or compromising that infrastructure ("cyber exploitation").[11] Cyberattacks may target government or private assets. They include efforts by states and non-state actors to damage and degrade computer software, hardware, and other aspects of computer operations, as well as to compromise cyber systems by infiltrating them without proper authority to obtain information or to control them in a variety of ways.[12] While some intrusions may not result in an immediate impact on the operation of a cyber system, as for example when a "Trojan Horse" infiltrates and establishes itself in a computer, such intrusions are considered cyberattacks when they can thereafter permit actions that destroy or degrade the computer's capacities.

---

[5]Admiral Dennis C. Blair, House Permanent Select Committee on Intelligence, *Annual Threat Assessment*, 111th Congress, 1st sess., 2009.

[6]Mike McConnell, "Mike McConnell on How to Win the Cyber-war We're Losing," *The Washington Post*, February 28, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493_pf.html (accessed on July 19 2010).

[7]See, for example, Evgeny Morozov, a Fellow at Georgetown University and a contributing editor to Foreign Policy, "Battling the Cyber Warmongers," Wall St. J., May 8-9, 2010, p. W3, col. 1, where he condemns "cyber-jingoism from former and current national security officials," including Richard Clarke and Mike McConnell, both of whom he notes are associated with security firms that have obtained or are seeking lucrative contracts with U.S. agencies and private firms. He refers to statements by Howard Schmidt that the notion of a "cyberwar" is "a terrible metaphor" and a "terrible concept." He acknowledges serious vulnerabilities but argues they stem largely from the incompetence of website managers and in any event do not require or justify the costly and privacy-restricting solutions being advanced by what he regards as alarmists.

[8]See generally the CSIS Commission Report on Cybersecurity, supra note 2; Richard Clarke and Robert K. Knave, *Cyber War: The Next Threat to National Security And What To Do About It* (New York: Harper Collins, 2010), 43-44.

[9]2009 Cyberspace Policy Review, 1. The Review quotes with approval the conclusion of the CSIS Commission Report, p. 11, that: "America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration."

[10]2009 Cyberspace Policy Review, i.

[11]"Cyberattack refers to deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks." National Research Council, "Cyberattack Capabilities", National Academy Press, Washington, D.C., 2009, p. 1.

[12]Id., 360-67. A listing of the sources of threats is compiled in the very useful GAO Report, "Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance," U.S. Government Accountability Office, Washington, D.C., 2010, p.4 (hereinafter "GAO July 2010 Report"): Bot-network operators; criminal groups; hackers; insiders; nations; phishers; spammers; spyware/malware authors; and terrorists. The Report also lists the "Types of Cyber Exploits" (p. 5).

Many forms of cyberattack have been identified, and new forms are continuously being devised. Among the cyberattacks of greatest concern are those conducted or supported by states and aimed at damaging or controlling cyber systems on which critical infrastructure depend, including power grids, air traffic control, and financial systems.[13] Many state and non-state actors seeking to attack or exploit U.S. cyber systems mask their identities by initiating their efforts from foreign countries, or by routing them through foreign computers and servers. Frequently, transnational attacks (some serious) are attributed to "patriotic" hackers, encouraged or tolerated by their governments.

Efforts to exploit cyber systems for the purpose of committing conventional crimes, or for other purposes regarded by states as harmful, are also common, and have caused significant losses and other costs. Cyber exploitation includes using the Internet and other cyber systems to commit fraud, to steal, to recruit and train terrorists, to violate copyright and other rules limiting distribution of information, to convey controversial messages (including political and "hate" speech), and to sell child pornography or other banned materials. Cyber systems contain vast amounts of data which criminals have been able to seize and utilize, such as Social Security numbers; and they enable criminals efficiently to approach millions of potential victims in attempted frauds and other schemes.

II. CURRENT CYBER-SECURITY MEASURES

The Internet currently is secured primarily through private regulatory activity, defensive strategies and products, national laws and enforcement, and some limited forms of international cooperation and regulation.

1. Private Measures

Non-governmental entities play major roles in the cyber security arena. Technical standards for the Internet (including current and next-generation versions of the Internet Protocol) are developed and proposed by the privately controlled Internet Engineering Task Force ("IETF"); the Web Consortium, housed at the Massachusetts Institute of Technology, defines technical standards for the Web. While the IETF was originally composed entirely of U.S. members, funded by and working for the U.S. government, it is today staffed entirely by volunteers, including network operators, academics, employees of private companies and government representatives. It establishes standards on a consensus basis. Membership and operations have become increasingly international, reflecting the growing interest of scholars, businesses, and governments throughout the world in the standard setting process.

Other privately controlled entities that play significant operational roles on aspects of cyber security include the major telecommunications carriers, Internet Service Providers ("ISPs"), and many other organizations, including:

- The Forum of Incident Response and Security Teams ("FIRST"), which attempts to coordinate the activities of both government and private Computer Emergency Response Teams ("CERTs") and is also working on cyber security standards;

[13]While state-sponsored attacks are often difficult to detect, for more than a decade states have used cyber warfare in retaliation to physical warfare or acts of aggression. In 1999, after a NATO jet bombed the Chinese Embassy in Belgrade, the Chinese Red Hacker Alliance launched a cyber assault on U.S. government websites. See Erbscholoe, Michael. Trojans, Worms and Spyware (NY: Butterworth-Heineman, 2005), 175. During the Second Chechen War, both sides engaged in cyber warfare with the Russian Federal Security Service responsible for knocking out key Chechen websites while Russian Troops engaged Chechen terrorists holding Russian civilians hostage. See Simons, Greg. Mass Media and Modern Warfare: Reporting on the Russian War on Terrorism (UK: Ashgate Publishing, 2010). During the Russia-Georgia war of 2008, the coinciding cyber assault was state-sponsored on both sides. There are suspicions that Iran and North Korea frequently promote state-sponsored cyberattacks though definitive evidence is often lacking. See Carr, Jeffrey and Shepherd, Lewis. Inside Cyber Warfare: Mapping the Cyber Underworld (Cambridge: O'Reilly Inc, 2009), 37. The GAO July 2010 Report (p.6) describes recent cyberattacks that illustrate potentially "debilitating impact on national security, " including a denial of service attack on Estonia (2007), an attack on DOD and other government computer networks (2008), attacks on California companies (2010), and attacks on Indian government computers (2009).

- The Institute of Electrical and Electronics Engineers ("IEEE"), which develops technical standards through its Standards Association and in conjunction with the U.S. National Institute of Standards and Technology ("NIST");
- The Internet Corporation for Assigned Names and Numbers ("ICANN"), which operates pursuant to a contract with the U.S. Department of Commerce (September 2009) transferring to ICAAN the technical management of the Domain Name System.[14]
- The International Electrotechnical Commission ("IEC") and the International Organization for Standardization ("ISO"), which together as non-governmental organizations, through their Joint Technical Committee, have developed information security standards for all types of organizations including one that addresses the development of information security management systems and the security controls that protect information assets (ISO/IEC 27001:2005);
- The European Telecommunications Standards Institute ("ETSI"), which is a non-profit, private entity with over 700 members from some 62 countries that produces through member-controlled committees globally applicable standards for Information Communications Technologies ("ICTs"), including for example the mobile Internet standards developed by its Third Generation Partnership Project ("3GPP");
- The Organization for the Advancement of Structured Information Standards ("OASIS"), another international, non-profit consortium that drives the development of e-business and web services standards through some 70 technical committees, and which did much of the work pursuant to UN request that led ultimately to an important, widely implemented standard, ISO 15000.

The standards promulgated by these bodies attempt to enhance security.[15] The standards are voluntary, however, in that the IETF and other, private standard-setting entities have no mechanism to mandate their use.

Protection from cyberattack and exploitation is primarily provided by private companies and individuals through passive, defensive measures: good software and equipment design, speedy and effective responses to weaknesses when identified, and the creation of various types of walls around systems or groups of users, including government agencies and public functions. ISPs and others responsible for infrastructure security invest in sound operational practices, redundant facilities, and other defensive measures that protect against most known forms of attack, but serious vulnerabilities exist (due among other things to inadequate maintenance and the failure of users to download patches), and new forms of attack are always being developed. Experts widely assume that attacks will be successful, and some believe that states, and perhaps other potential attackers, could, if they chose, inflict major damage on cyber systems and their dependent infrastructure.[16]

Security measures must be cost effective to get accepted. While the IETF has, for example, published standards that would, if adopted, increase the security of the Domain Name System ("DNS"), operators of the ".com domain" failed for a considerable period to turn on these protocols, claiming their implementation would double the infrastructure needed to handle the resulting increased message size.[17]

[14]ICANN is nominally a private, U.S., not-for-profit corporation, but is widely seen as U.S. controlled. It performs the functions of the Internet Assigned Names Authority, through which it establishes standards for the use and protection of names used in cyber communications. While it has some enforcement powers, it has thus far limited its exercise of powers to determining which entities are entitled to use which names, and has no useful authority to defend cyber systems from attack by individuals or groups prepared to disregard its rulings.

[15]We describe below specific examples of security-related IETF standards, such as secure BGP, IPSec, DNSSEC, RPKI, and encryption. More generally, all proposed IETF standards must include a security analysis as part of their specification.

[16]Clarke and Knave, 92. The authors anticipate that "logic bombs"—software that erases all programming, effectively negating further use of a device—will be used in attacks and may already be in place.

[17]DNS security flaws were identified in the early 1990s. Efforts to include security mechanisms led to the design of Domain Name System Security Extensions ("DNSSEC"), initially laid out in RFC 2535, an IETF paper. Despite being available for many years, DNSSEC is not more widely used because of backward compatibility issues, implementation costs, and perceived complexity of switching protocols. DNSSEC specifications (laid out in RFC 2535) have since been updated to make implementation more practical; See RFC 4033, 4034, and 4035 for updated DNSSEC-*bis* specifications.

Negligence by users also leads to costly breakdowns in defense. Victims, especially companies whose businesses depend on secure cyber activities, frequently fail to report flaws and successful attacks in order to avoid damaging their reputations. This in turn results in slower responses to attacks and greater damage. Inadequate sharing of information is a serious impediment to effective defense.

2. National Measures

Many national governments have adopted laws aimed at punishing and thereby deterring specific forms of cyberattacks or exploitation. The U.S., for example, has adopted laws making criminal various forms of conduct, including improper intrusion into and deliberate damage of computer systems.[18] These laws have little or no effect, however, on individuals, groups, or governments over whom the U.S. lacks or is unable to secure regulatory or criminal jurisdiction.

US national security experts almost exclusively emphasize the need for national measures for enhancing cyber security. They recommend national laws to protect the sharing of information about threats and attacks; methods for government bodies, such as the NSA, to cooperate with private entities in evaluating the source and nature of cyberattacks; and more effective defenses and responses to cyberattacks and exploitation developed through government-sponsored research and coordination pursuant to cyber security plans. Efforts of this sort are underway, and the U.S. government is examining what strategic defenses can be developed and utilized to protect critical infrastructure that depend upon vulnerable cyber systems.[19]

The GAO's July 2010 report details the specific roles being played by many U.S. agencies in efforts to enhance "global cybersecurity," but ultimately concludes that these efforts are not part of a coherent strategy likely to advance U.S. interests. It considers the National Security Council ("NSC") the "principal forum" for all national security matters requiring presidential involvement, and notes (p. 18) that the NSC's Information and Communications Infrastructure Policy Committee ("ICI-IPC"), created in March 2009, approved a subcommittee on "international cyberspace policy efforts (the International sub-IPC) composed of officials from the Departments of Commerce, Defense, Homeland Security, Justice, State, and Treasury, the Office of the U.S. Trade Representative, and the Federal Communications Commission. It describes the many functions performed by each of these agencies, including their participation in standard setting discussions, and in the work of international agencies such as the ITU and its study groups. (For each of the agencies the GAO provides a list of "efforts" in the form of tables to its report.) Many of the functions listed involve defensive preparations or investigation and prosecution for cyberattacks and exploitation. U.S. agencies engage in discussions in many international groups. But these activities have little significance, the GAO concludes, as they are not coordinated aspects of a plan but rather ad hoc "engagement" with other countries and groups. The GAO concludes (p. 32) that, as of the time its study was conducted, the U.S. lacks top-level leadership (the International sub-IPC does nothing more than ensure that all agencies are aware of each others' international activities), and that while multiple agencies are involved "in a variety of international efforts that impact cyberspace governance and security, the U.S. government has not documented a clear vision of how these efforts, taken together, support overarching national goals." It notes that officials from the Departments of State and Defense told the GAO that "an effort is currently under way to develop an international strategy for cyberspace," but concludes: "we have not seen any evidence of such activities . . . ." It also found that, even with regard "to information-sharing or incident response agreements with other countries, the federal government lacks a coherent approach toward participating in a broader international framework . . . ." This is due in part to national security concerns, and the Report notes (pp. 35-36) a comment by

[18]E.g., *Fraud and Related Activity in Connection with Computers*, U.S. Code 18, § 1030.

[19]The Wall Street Journal reported on an NSA program, through Raytheon, Corp., called "Perfect Citizen," to provide a "cyber shield" for critical infrastructure such as the electricity grid and nuclear power companies, that currently depend on insecure computer networks. The program is voluntary and part of the Comprehensive National Cyber-security Initiative, which is itself classified. July 8, 2010, p. A3.

a DOD official "that there is disagreement, particularly within the U.S. intelligence community, as to whether the benefits of showing cyber-threat information outweigh the risk of harm to U.S. security interests should sensitive data be leaked to an adversary of the United States."

3. International Measures

National governments often cooperate with each other informally by exchanging information, investigating attacks or crimes, preventing or stopping harmful conduct, providing evidence, and even arranging for the rendition of individuals to a requesting state. States have also made formal, international agreements that bear directly or indirectly on cyber security. Extradition treaties generally apply to a list of activities that constitute crimes in the states that agree to arrest and/or extradite individuals to each other. Mutual Legal Assistance Treaties ("MLATs") also generally apply to a list of agreed crimes; they require state parties to assist one another by providing information, evidence, and other forms of cooperation when requested to do so in such situations. These international agreements apply to the criminal activities specified, including situations in which the alleged criminals have used cyber systems in those activities.

International agreements that potentially bear upon cyber-security activities also include treaties (the UN Charter and Geneva Conventions) and universally accepted rules of conduct (customary law). Cyberattacks that have kinetic effects equivalent to a physical use of force, for example, are likely to be considered "armed attacks" under the UN Charter to the same extent as physical uses of force. The U.S. is reported to have proposed this concept as a governing principle in discussions with Russia and other states.[20] In addition, the right of states to exercise self-defense or to take countermeasures in response to such attacks would depend on their potential consequences. International law also provides rules related to the use of force during armed conflict that presumably apply to cyberattacks, including for example requirements that noncombatants and civilian institutions such as hospitals not be deliberately attacked, and that uses of force be restricted to measures that are necessary and proportionate. Considerable uncertainty exists, however, as to the application of rules written to regulate physical force to uses of cyberforce, and the issues are further complicated by the fact that the scope of use-of-force rules is far from universally agreed.

The most significant, multilateral arrangement that specifically addresses aspects of cyberattacks and exploitation is the Council of Europe Convention on Cybercrime ("CEC"). The CEC is a law-enforcement treaty designed to develop a common criminal-law policy aimed at defining, punishing, and thereby deterring cyber-related crimes. It requires all Member States (46 had signed and 30 had ratified as of June, 8th, 2010)[21] to adopt laws making criminal the following five types of actions against the integrity of cyber systems: illegal access; illegal interception; data interference; system interference; and misuse of devices. It also identifies types of conduct involving exploitation of cyber systems that Member States agree to make criminal, including fraud, forgery, child pornography, and violations of copyright laws. States are allowed to exempt from prosecution for some of these activities individuals who act without intent to harm. Member States are required to provide their domestic law enforcement agencies with the authority to investigate the covered conduct, and to cooperate with other Member States in their enforcement through extradition treaties and MLATs. States are entitled to make reservations that exempt themselves from prosecuting particular crimes, and to withhold cooperation in cases deemed inconsistent with their public policies or security.

The CEC's potential in providing cyber security is limited by the fact that its "law enforcement framework operates in many cases on a time scale that is too long to protect victims of cyberattack from

[20]John Markoff, "Step Taken to End Impasse Over Cybersecurity Talks," New York Times, July 17, 2010, A7, col. 1: "'The U.S. put forward a simple notion that we hadn't said before,' the diplomat said. 'The same laws that apply to the use of kinetic weapons should apply to state behavior in cyberspace.'"

[21]See Convention on Cybercrime CETS No. 185 at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=&CL=ENG.

harm."[22] The CEC is no more effective in preventing cyberattacks than criminal law enforcement is in preventing conventional attacks. The treaty has no mechanism, moreover, for establishing or revising cyber-system practices or standards that could generally improve security. Furthermore, the CEC's potential in securing universal adherence is diluted by its inclusion of efforts to punish conduct based on content restrictions (such as fraud and child pornography) rather than focusing on efforts to punish cyberattacks that potentially damage the cyber infrastructure itself. Its limitations on "hate" speech seek to regulate an area in which states have strong differences, ranging from policies prohibiting all political speech to prohibiting only speech amounting to illegal conduct.

Another international agreement of significance is the Shanghai Cooperation Organization's ("SOC") set of principles or "action plan" related to Information Security adopted at the SOC's Seventh Council Meeting of Heads of State (China, Russia, Kazakhstan, the Kyrgyz Republic, Tajikistan and Uzbekistan) held on August 16, 2007 in Kyrgyz. The SOC principles are consistent with the law-enforcement approach of the CEC insofar as they relate to securing cyber systems from attack, but they differ markedly from the CEC by stressing the Members' intent to ensure national control over cyber systems and content. The agreement is signed by its six Member States, and like the CEC is open to approval by other states. The SOC principles confirm Member State control over the content of cyber communications, including any speech considered politically destabilizing.[23]

Many established international regimes have addressed or are considering cyber security issues. The CSIS Commission on Cybersecurity for the 44th Presidency noted the need to deal proactively with these efforts. The 2009 Cyberspace Policy Review notes that some of these efforts could result in regulations that overlap or conflict with each other, citing as an example the simultaneous development of forensics standards by both the International Telecommunications Union ("ITU") and the International Standards Organization ("ISO").[24] The GAO's July 2010 report strongly supports these conclusions, stating (pp. 36-37): "the sheer number of international entities engage in incident response can also impede international coordination." It provides several examples of the difficulties of working with states (even in Europe) and with CERTs, and concludes that coordinating bodies such as FIRST and the UN-created Global Response Center lack the demonstrated capacity "to provide a legitimate global information security service to benefit all participants . . . ."

These conclusions seem correct and significant, but they appear to understate the scope and intensity of current international activities that are taking place regardless of U.S. involvement, including in particular the ITU's plans.[25] Acting pursuant to annual calls by the UN General Assembly for greater international cooperation in dealing with cyber threats, and after numerous conferences and studies by a variety of private, national, regional and international groups, the ITU convened a World Summit on the Information Society ("WSIS") at which governments and world leaders called on the ITU to become the sole "Facilitator of Action" in what was designated Action Line 5: "Building confidence and security in the use of ICTs [Information and Communications Technologies]." After a series of meetings, declarations, programs, and considerable effort by experts and supporting governments, the ICT launched on May 17, 2007 and announced in 2008 its Global Cybersecurity Agenda ("GCA") "to provide a framework within which an international response to the growing challenges to cybersecurity can be coordinated and addressed." The GCA stresses the desirability of a concerted effort by all stakeholders "to build con-

[22]National Research Council, "Cyberattack Capabilities," 62.

[23]See ITU GCA, Global Strategic Report, 21.

[24]2009 Cyberspace Policy Review, 20-21.

[25]The ITU's Global Strategic Security Report (last update June 2008) summarizes the activities and "legislative" measures of regional organizations, including in addition to the CEC actions and declarations by the G8, the European Union, the Asian Pacific Economic Cooperation (which has an active Telecommunications and Information Working Group), the Organization of American States, the Commonwealth, the Association of South East Asian Nations, the Arab League, the African Union, and the Organization for Economic Cooperation and Development. See ITU Global Cybersecurity Agenda, "Global Strategic Report" (2009): 16-21. The Global Strategic Report is available at http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html (accessed July 23, 2010).

fidence and security in the information society," but it sees the ITU as "uniquely placed" to be the lead agent in this effort. The ITU has 191 Member States and more than 700 Sector Members, and its sectors of operations (Radiocommunication, Standardization, and Telecommunication Development) are being rapidly expanded to include cyber-related issues. It is pursuing its perceived role through a broad range of activities in cyber security education and in the development and promulgation of a comprehensive array of plans and protocols intended to create a secure cyber infrastructure by dealing with cyber crime, technical standards, security requirements, capacity building, and even the promotion of child on-line safety.[26] The GCA calls for continued involvement of all existing stakeholders in the cybersecurity effort. At the same time, however, it clearly signals its determination to seek the implementation of standards issued by its own standards development body (ITU-D) and by the ISO, as well as its intention to play the leading if not the sole coordinating role in all aspects of cybersecurity.

Numerous other governmental entities play, or purport to play, significant roles on international cyber security issues. Various regional bodies have cybersecurity working groups, including the Asia-Pacific Economic Cooperation (APEC), the Association of Southeast Asian Nations (ASEAN), the European Union (EU), the Group of Eight (G8), the Organization of American States (OAS), and the Organization for Economic Cooperation (OECD). The North Atlantic Treaty Organization (NATO) has several defense-related cyber operations. INTERPOL, with 188 members, focuses on cyber crime and assists in investigations. Some of these entities go beyond merely discussing problems and seek to develop policies and standards to enhance security. The Meridian Conference and Process, founded in 2005, hosts government discussions regarding critical infrastructure protections. Any international negotiation will have to take into account the work of these and other governmental (and non-governmental) organizations that have become active in cyber-security issues, especially the claims and activities of such entities as the ISO and ITU.

III. POTENTIAL FOR INCREASED INTERNATIONAL COOPERATION AND REGULATION

The current, largely unilateral and defensive measures relied upon to provide cyber security in the U.S. (and elsewhere) are widely viewed as insufficient to ensure an adequate level of safety.[27] It may be possible, as CSIS and others have recommended, to provide adequate protection for certain, critical national security activities by isolating them from the Internet and other outside interventions. For most, current functions, however, some aspects of the principal security deficiencies identified can only be remedied or reduced through increased and more effective international cooperation.

The first recommendation for a multilateral treaty to deal with cybersecurity was published by Stanford University's Center for International Security and Cooperation in 2000. That draft proposed creating an international agency with regulatory authority similar to that of established specialized

[26]The measures listed in ITU reports include assistance to states in developing national cybersecurity strategies; the "ITU Toolkit for Cybercrime Legislation" and its study "Understanding Cybercrime"; several technology and security standards issued by ITU Study Group 17, which it calls "the lead study group on telecommunications security and identity management," a status the ITU notes was "confirmed by the ITU-T World Telecommunication Standardization Assemblies (WTSA) in 2000, 2004 and 2008, in close collaboration with ISO/IEC, as a tripartite joint action." In addition to numerous specific cyber-related standards that the ITU-T has issued (including for example its H.235.x series of recommendations for security infrastructure and service including authentication and privacy) is what it calls its ICT Security Standards Roadmap, which it states "promotes the development of security standards by highlighting existing standards, current work and future standards among key standards development organizations." See generally the ITU's GCA brochure and extensive materials available at http://www.itu.int/osg/csd/cybersecurity/gca/ (accessed July 23, 2010).

[27]The NRC "Cyberattack" report (39-40) notes that cyberattack capabilities are relatively inexpensive and increasingly available to both governments and non-state actors, and notes the inherent weaknesses of passive cyberdefense, "exploitable vulnerabilities will continue to be present in both civilian and military computer systems and networks of the United States. Thus, the U.S. information infrastructure is likely to remain vulnerable to cyberattack for the foreseeable future, . . . [C]yberconflict is quite unlike the land, air, and maritime domains in which U.S. armed forces operate, and enduring unilateral dominance with respect to cyberconflict is not realistically achievable by the United States."

agencies in other areas of transnational activity, but with heavy reliance on private expertise. It expressly excluded state action from its scope.[28] The U.S. has opposed such an approach, but support for multilateral understandings and activities has increased.[29]

General Assembly ("GA") resolutions commencing in 1998 (GA Res. 53/70) have been adopted annually, noting various aspects of the cyber security problem including crime, terrorism, critical infrastructure protection, spam, attacks on cyber infrastructure, and the need for capacity building.[30] In addition, conferences supported by the UN, individual governments, regional organizations, and others have been held on several occasions at various places in the world, resulting in calls for increased international cooperation to deal with threats to cyber security.[31] On January 6, 2006, the GA adopted Resolution 60/45, calling among other things for the appointment by the Secretary General of "a group of governmental experts, to be established in 2009 on the basis of equitable geographical distribution," to continue to study "existing and potential threats in the sphere of information security and possible cooperative measures to address them," and "to submit a report on the results of this study to the General Assembly at its sixty-fifth session." The Group of Governmental Experts representing 15 states, including China, India, Russia, and the U.S., met four times and on July 10, 2010 issued a report summarizing the threats currently faced by Information and Communication Technologies ("ICTs"), and recommending the following "further steps for the development of confidence-building and other measures to reduce the risk of misperception resulting from ICT disruptions":

1. Further dialogue among States to discuss norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructures;
2. Confidence-building, stability, and risk reduction measures to address the implications of State use of ICTs, including exchanges of national views on the use of ICTs in conflict;

---

[28]Abraham D. Sofaer and Seymour E. Goodman, "A Proposal for an International Convention on Cyber Crime and Terrorism," (CISAC, Aug. 2000) (with the assistance of several other scholars) (hereinafter "Stanford Draft"). Any current treaty should not be limited to "crime" and "terrorism" but rather should address cyber security in general.

[29]Dartmouth's Institute for Information Infrastructure and Protection issued a report in 2009, *National Cyber Security Research and Development Challenges,* addressing the international issues and calling for a multilateral international agreement:

> While there are U.S. laws and regulations that address physical border concerns, the issues become far less clear in the borderless reality of cyberspace. One participant observed, ". . . a world protocol is needed. We have a world economy, a world legal system . . . For information security, we need world conduct, ethics, monitoring, and response. The U.S. cannot do it alone." The object of the international doctrine should be to devise ways to eliminate threats, not just to identify ways to defend against them. Such a doctrine should specify clear roles and responsibilities regarding the security of IT components, from producers to customers. Moreover, the doctrine should codify normative behavior in cyberspace and should identify cyber attacks and abuse as crimes rather than national security issues.

Richard A. Clarke and Robert Knake call for a treaty modeled after the Strategic Arms Limitation Treaty (SALT) to address cyber war. They propose a "Cyber War Limitation Treaty, or CWLT" that would "establish a Cyber Risk Reduction Center. . . . coordinate with the United Nations . . . exchange information and provide nations with assistance . . . create international law concepts [for example] the obligation to assist and national accountability . . . ban first-use cyber attacks. . . . " They also call for banning cyberattacks on civilian infrastructure. In order to address the problem of non-state actors, they propose that the treaty "shift the burden of stopping them to the states party to the convention." Richard A. Clarke and Robert K. Knake, *Cyber War* (New York: Harper Collins 2010), 270.

[30]Among the most important of several General Assembly Resolutions on this subject is No. 55/63. It recommends: establishing a set of universally agreed principles for the use and protection of cyberspace; understandings by governments as to their responsibilities regarding their resort to cyberattacks or investigations; agreements by governments as to private activities that should be prohibited to enhance cyber security; commitments by governments to criminalize, prevent, investigate, prosecute and punish such activities; commitments by governments to provide forensic cooperation in cyber investigation and prosecutions by other governments, and to extradite or prosecute violators of agreed norms; agreements among states to allow within their territories certain types of investigation of cyberattacks by other governments; consideration and implementation through an agreed entity of protocols and standards designed to enhance cyber security; and the collective development and funding of an effective, multilateral program of support for cyber competence and capacity throughout the world to facilitate development and economic growth while instilling proper practices.

[31]In addition to the many ITU resolutions on the subject, the GCA report summarizes other, significant conferences held on related subjects at 22-23. The GAO July 2010 Report (pp. 8-17) also provides considerable, useful information on such transnational activities.

3. Information exchanges on national legislation, national ICT security strategies and technologies, policies and best practices;
4. Identification of measures to support capacity-building in less developed countries; and
5. Finding possibilities to elaborate common terms and definitions relevant to United National General Assembly resolution 64/25.[32]

This set of recommendations is far from a major step toward a cyber security treaty. Nonetheless, the report represents a breakthrough in the deadlock that had developed due to demands by some states for sweeping cyber security agreements, related especially to armed conflict, and U.S. opposition to international negotiations on cyber warfare and other aspects of cyber security. The willingness of the U.S. to begin discussions on state conduct, norms, defensive strategies, best practices, and capacity building represents a significant shift in national policy. It apparently results from the Obama Administration's willingness to consider international measures to enhance deterrence through international cooperation. Its 2009 Policy Review concluded that "International norms are critical to establishing a secure and thriving digital infrastructure," and that the U.S. should formulate its positions internally and attempt to implement them in all appropriate international forums.[33] While prior U.S. government policy pronouncements recognized a general need for international cooperation, the 2009 Policy Review specifically recommends that the U.S. government, working with the private sector, "should coordinate and expand international partnerships to address the full range of cybersecurity-related activities, policies, and opportunities associated with the information and communications infrastructure . . . ."[34]

Members of Congress, too, have signaled increased support for international cooperation to enhance cyber security. A 2009 GAO Report on national cybersecurity strategy called for an international agreement and a global cyber strategy.[35] In September 2009, Senator Dianne Feinstein called for an international agreement regulating cyber warfare much like regular warfare:

> In addition, the government must consider that effective cyber security inside the United States will require stronger diplomatic efforts and an international agreement on what will and will not be tolerated in cyberspace. An international framework on cyber warfare, much like international conventions on traditional warfare, is needed to govern this rapidly growing field.[36]

On July 10, 2009, Senator Kirsten Gillibrand introduced legislation that would encourage the Secretary of State to work with governments of other countries to coordinate cooperation on cybersecurity, and would require a report to Congress on the progress of those efforts.[37] On March 23, 2010, Senator

[32]Item 94 of the provisional list (A/65/100), "Developments in the field of information and telecommunications in the context of international security."

[33]*2009 Cyberspace Policy Review*, iv.

[34]*2009 Cyberspace Policy Review*, 20-21. The 2009 Cyberspace Policy Review, consistent with prior reports, places primary emphasis on domestic measures in its proposed plan to improve cyber security; it also refers, however, to the need for greater international cooperation and efforts, based on its conclusion that (17): "The global challenge of securing cyberspace requires an increased effort in multilateral forums . . .—in continued collaboration with the private sector—to improve the security of interoperable networks through the development of global standards, expand the legal system's capacity to combat cyber crime, continue to develop and promote best practices, and maintain stable and effective internet governance."

[35]U.S. Government Accountability Office, *National Cybersecurity Strategy*, testimony prepared for Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, 111th Cong., 1st sess., 2009, GAO-09-432T. The GAO has since then published two reports bearing directly on international cooperation and cyber security. Its March 2010 report—"Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative," GAO-10-338 (Washington, D.C.)—concluded that the U.S. lacks a formal strategy for coordinating outreach to international partners for standards setting, law enforcement, and information sharing. Its July 2010 Report, referred to at various points in this paper, reaffirms that conclusion on the basis of a comprehensive study of national and international activities.

[36]Senator Diane Feinstein of California, speaking for the Senate Resolution Supporting the Goals and Ideals of National Cybersecurity Awareness Month and Raising Awareness and Enhancing the State of Cybersecurity in the United States, on September 24, 2009, to the Senate, S. Res. 285, 111th Cong., 1st sess., *Congressional Record* 155 (September 24, 2009): S 9852-3.

[37]For the Senate bill, see *International Cybercrime Reporting and Cooperation Act*, S 3155, 111th Cong., 2nd sess., *Congressional Record* 156 (March 23, 2010): S 1873.

Gillibrand joined with Senator Orin Hatch to propose a more comprehensive bill coordinating global cybersecurity efforts. In a statement supporting the bill, Senator Hatch announced:

> Cybercrime is a tangible threat to the security of the global economy, which is why we need to coordinate our fight worldwide. Until countries begin to take the necessary steps to fight criminals within their borders, cybercrime havens will continue to flourish. We do not have the luxury to sit back and do nothing, and the International Cybercrime Reporting and Cooperation Act will not only function as a deterrent of cybercrime, but will prove to be an essential tool necessary to keep the Internet open for business. Countries that knowingly permit cybercriminals to attack within their borders will now know that the U.S. is watching, the global community is watching, and there will be consequences for not acting.[38]

The Senators announced that their bill had the support of such U.S. companies as Cisco, HP, Microsoft, Symantec, PayPal, eBay, McAfee, and major financial institutions.[39]

IV. FASHIONING EFFECTIVE INTERNATIONAL INITIATIVES

The potential advantages of securing agreements on international norms and standards related to cyber security stem from the view that states could by adopting and implementing such measures create a culture and practices more favorable to cyber security than currently exist. The important insight that the Internet and other cyber systems are (like other transnational activities) subject to state control,[40] implies that state support is necessary to achieve effective security norms and appropriate technology standards. Only states can limit their own destabilizing activities, and their cooperation is essential to curb so-called patriotic hackers and cyber crime. Harmonization of laws and practices cannot assure effective cooperation, particularly in enforcing rules or practices that fail accurately to reflect underlying differences in policy. But harmonization has not occurred and is essential to secure the benefits of criminal law enforcement through extradition treaties and MLATs, and to achieve interoperability of security systems. Harmonization, effectively applied, implies the existence of national plans and practices that enable the implementation of common international policies.

An enhanced capacity to implement norms, practices, and standards is another potential benefit of an international arrangement. Assuming—as we do—that the current, privately and professionally controlled process for reaching common technology positions on cyber activities is valuable and worth preserving, a mechanism whereby national governments could concur in such positions through an international structure could serve to achieve faster and more uniform acceptance, resulting in more secure and robust cyber networks. Finally, an international arrangement could serve to resolve some if not all the current political maneuvering over what agencies, states, or other entities should perform key transnational roles in ICT development and security. The current, de facto distribution of power appears to have ignited a competition for influence likely to disrupt rather than to enhance cyber security. An agreed redistribution of responsibilities that is acceptable to all stakeholders could ensure constructive cooperation in a highly complex undertaking.

But negotiating agreements that effectively exploit these potential advantages must satisfactorily address the difficulties and objections that thus far have led the U.S. (and others) to refrain from seeking international agreements beyond the CEC. Not all aspects of cyber insecurity are currently susceptible to international agreement. Some seem beyond the reach of acceptable resolution because the issues are novel or intractable. Others reflect major policy differences among potential member states concerning freedom of speech, privacy, or other social and political values. Others stem from the underlying premise that U.S. interests are inconsistent with international cooperation. Some states (including the U.S.) are

[38]Senator Orrin Hatch of Utah, speaking for the International Cybercrime Reporting and Cooperation Act, on March 23, 2010, to the Senate, S. 3155, 111th Cong., 2nd sess., *Congressional Record* 156 (March 23, 2010): S 1876.

[39]"Hatch, Gillibrand Introduce First of its Kind Measure to Bolster Cybersecurity," Orrin G. Hatch Newsroom, the Senator's Press Releases, March 23, 2010, http://hatch.senate.gov/public/index.cfm?FuseAction=PressReleases.Detail&PressRelease_id=8bcbfb97-1b78-be3e-e0e3-58aed09a749a&Month=3&Year=2010 (accessed July 21, 2010).

[40]Jack Goldsmith and Tim Wu, Who Controls the Internet: Illusions of a Borderless World (Oxford Press 2008).

as yet unwilling to be bound by limitations that their public complaints suggest they believe should bind others. Many U.S. officials and experts may in fact believe that U.S. security would be diminished through international cooperation rather than enhanced. Sharing information on cyber vulnerabilities, even with allies, could result in exposing those weaknesses to states prepared to exploit them. Sharing and improving the defensive capacities of all states would result in strengthening those whose networks the U.S. itself may seek to penetrate for intelligence or other purposes. Finally, even where agreement may be possible that an area of cyber activity is a likely subject of international agreement, the measures that are appropriate for that purpose will vary, and the form of the entity assigned the task of implementing those measures must also be agreed.

These difficulties and objections present real and challenging obstacles to international cooperation. They cannot be overcome by invoking sweeping generalities about the values of international cooperation. They do not, however, preclude international agreements on many aspects of cyber security. Rather, they reflect objections based on national security, political, and ethical concerns that are familiar from other areas of international engagement, and that can be effectively managed by adopting parameters for cyber agreements fashioned with due regard for such concerns. The U.S. pursues agreements in such areas, despite the risks, when they are expected to confer security and/or economic benefits. A useful example (based on incidents described in the GAO July 2010 Report, pp. 34-35) is the vigorous and successful effort by the U.S. Trade Representative to use international trade agreements as the basis for preventing China in 2007 from regulating (through testing and certification) the commercial sale of products such as routers, smart cards, secure databases and operating systems, and for convincing South Korea to drop a plan to mandate an indigenous encryption standard as part of a large-scale government adoption of voice-over-Internet Protocol systems. To the extent the U.S. adopts stringent cyber security standards for commercial sales of products, or otherwise erects cyber security-related trade barriers, it should expect that it will be unable to convince other states to open their markets to U.S. sales in similar circumstances. The optimal policy in such situations is to restrict those transactions that national security truly demands, while accepting and managing lesser risks where they are outweighed by countervailing advantages.

An appropriate approach would, taking into account such concerns, (1) limit at least initial efforts to **areas of activity** that are appropriate subjects for international cyber-security agreements; (2) determine and specify the **types of measures** that member states should undertake concerning each of the activities they include in such agreements; and (3) fashion the **administrative structure and functions** of any entity that should be utilized for this purpose in a manner that preserves what currently works well while improving what does not.

1. Determining the Activities to Include or Exclude from International Arrangements

International regulatory regimes regularly specify the areas of activity to which they apply or are considered inapplicable. The International Civil Aviation Organization ("ICAO"), for example, pursuant to the Chicago, Montreal, and other conventions, regulates civil aviation but has no authority over military aircraft and activities. Such limitations are common in international agreements, and are often necessary to attract the widespread support required for potentially meaningful cooperation.

The following areas of cyber activities are likely to be excluded from an international agreement at this time, or to be included only to a limited extent: (a) aspects of **cyber war**; (b) **cyber intelligence**; (c) politically related **content restrictions**; (d) proposals that unacceptably limit **privacy or human rights**; and (e) other concerns that states believe may prejudice their **national security** interests. This is not to say that these areas of activity should be ignored, but rather that they should be approached with an awareness of their likely sensitivity and correspondingly modest expectations.

(a). Cyber War

Cyber "war" is an area of great, public concern, and several proposals have been made to limit, or even to prohibit, cyber warfare. Russia proposed several years ago that all forms of cyber warfare

be outlawed. China refused to accept so sweeping a restriction, viewing cyber warfare as an arena in which it could be successful in competing with the U.S. and other militarily powerful states. The U.S. for years indicated it was uninterested in even discussing limitations on cyber warfare. Military officials assigned leading roles in developing U.S. cyber capacities in fact announced their intent to "dominate" cyberspace.[41] The U.S. has created a Cyber Command, reflecting its view that cyber space is a new theater for national security activities analogous to the ground, sea, or air theaters of operations. Other states are responding to these developments by building their own capacities to engage in defensive, retaliatory, or anticipatory measures aimed at deterring or preventing cyberattacks.

The notion that the U.S. or any other state will be able to "dominate" cyber space seems unlikely ever to be correct. The use of such rhetoric—coupled with the announcement (uncoordinated with the Department of State) of the creation of a Cyber Command—has undoubtedly led other states to regard U.S. military policy as posing a threat to which they must respond. The critical response to this inflammatory posture may have led the U.S. recently to indicate for the first time an interest in pursuing agreements on cyber war issues. At his Senate confirmation hearing on April 15, 2010 to be Director of the NSA and Commander of the newly created U.S. Cyber Command, Lieutenant General Keith B. Alexander, said: "This command is not about efforts to militarize cyber space. Rather, it is about safeguarding the integrity of our military's critical information systems."[42] And in the UN sponsored Expert Group report, issued on July 17, 2010, the U.S. joined 14 other states, including China and Russia, in agreeing to consider "confidence-building, stability, and risk reduction measures to address the implications of State use of ICTs, including exchanges of national views on the use of ICTs in conflict."

Reaching agreement on cyber-war related issues will be difficult. The activities potentially covered by the concept of cyber warfare are numerous and important to the national security of potential member states. Furthermore, cyber capacities permeate modern warfare, and their use in armed conflict is already extensive and indispensable. The extent to which cyberattacks should or could realistically be treated as equivalent to conventional armed attacks is unclear. Individual computers could not reasonably be treated as analogous to conventional weapons. Verification of the performance of commitments would be difficult if not impossible. And violations would, absent some new forms of monitoring, remain difficult to trace and attribute to particular states.[43]

Despite these difficulties, agreements may be possible about specific aspects of cyber warfare. As the present NRC Committee's Letter Report notes, conventional arms control agreements may restrict the number, type, or use of weapons, may require advance notice of activities, and may establish rules limiting appropriate targets.[44] Agreements could be reached, for example, that apply certain established international-law principles to cyberattacks, as suggested recently by a U.S. diplomat familiar with the Expert Group negotiations. Governments would probably agree that a cyberattack by the armed forces

[41]Clarke and Knave, 41-44.

[42]Senate Committee on Armed Services, *Nomination of VAdm James A. Winnefeld, Jr. USN, to be Admiral and Commander, U.S. Northern Commander, North American Aerpospace Defense Command; and Ltg. Keith B. Alexander, USA, to be General and Director, National Security Agency/Chief, Central Security Service/Commander, U.S. Cyber Command, 111th Cong. 2nd sess., April 15, 2010*, 9. Chairman Carl Levin described in his statement at the hearing the need for caution by the U.S. in resorting to cyberattacks (3): "Coupled with the fact that the United States economy and government are the most dependent in the world on the Internet and are therefore the most vulnerable to attacks, the Nation must not only invest in the effectiveness of its defense, but think carefully about the precedents that it sets, hopefully acting wisely in ways that we will accept if others act in the same or similar ways." He said the committee had been "assured that the Department of Defense leadership and the administration as a whole is committed to rapidly closing the cyber space policy gap. The committee has also been assured that the Defense Department is proceeding with appropriate caution and care regarding military operations in cyberspace."

[43]Comprehensive discussions of the application of existing international law to cyber warfare include the paper prepared for the current NRC study by Michael Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense and Armed Conflicts" (NRC, 2010); and Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," published in the *Berkeley Journal of International Law* (*BJIL*), Vol. 25, No. 3.

[44]National Research Council Committee on Deterring Cyber Attacks, *Letter Report for the Committee on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy* (March 25, 2010), http://www.nap.edu/catalog/12886.html (accessed July 23, 2010).

of a state, with kinetic effects on the territory of another state equivalent to those of a conventional armed attack, should be treated in the same manner as a conventional attack, giving rise to the right of individual and collective self-defense, and allowing upon proper attribution resort to both cyber and kinetic responses. States could also confirm that targets normally immune during armed conflict from conventional attack, such as medical services and religious institutions, are also immune from cyberattacks. They could even agree that potentially appropriate targets during armed conflict, such as power grids, food supply, and financial infrastructure, should be immune from cyberattack under all circumstances.

One method for accomplishing limits on military activities (i.e., cyber war) without attempting directly to regulate national forces is exemplified by the protections established for civilian aircraft. The Chicago Convention (Art. 3) provides that it "shall be applicable to civil aircraft, and shall not be applicable to state aircraft"; and it also recognizes (Art. 1) "that every State has complete and exclusive sovereignty over the airspace above its territory." The Convention also, however, requires contracting states to issue regulations for their state aircraft "that they will have due regard for the safety of navigation of civil aircraft," an obligation that effectively limits the use of force other than in armed conflict (expressly excepted in Art. 89), and it grants certain qualified but significant rights of passage over the territories of all contracting states even to nonscheduled flights (Art. 5).[45] It may be possible, by analogy, to limit "cyber war" implicitly if not explicitly by granting protections to specified cyber activities or assets.

Identification protocols would likely be necessary to establish for protected entities or functions. Doing so in a manner that effectively limits abuse will pose problems, as states or groups having access to such protocols may use the information to target the entities and functions sought to be protected. The problem of accurate attribution of illegal cyberattack may tend to diminish the normal deterrent effect of potential uses of force in self-defense. Non-state actors may be particularly inclined to risk illegal attacks, since they lack corresponding institutions. A system for determining responsibility and imposing remedies, including monetary damages, against not only states but also ISPs and other responsible parties, could be a helpful supplement to responsive uses of force. But here, too, the difficulties will be substantial. International tribunals have lost their appeal. Furthermore, imposing damages on states for military activities is rarely acceptable other than on a voluntary (ex gratia) basis, and the threat of civil liability is likely to have no effect at all on non-state actors prepared deliberately to attack civilian infrastructure.

Considerable planning and negotiation will have to take place both within and among potential parties before progress can be expected on most cyber-war issues. While much public attention and official concern has been expressed about the dangers of cyber war, the U.S. will not be prepared to seek legal limits on such activities until it has determined that it is prepared to accept reciprocal obligations. No internal review has yet been made as to the cyber-war policies the U.S. should adopt or advocate in the international arena. Even after the U.S. has resolved internally its international cyber warfare policies, the appropriate, initial forum for implementing such policies may be with U.S. allies, in NATO for example, rather than through a multilateral arrangement with states that have different agendas and are less trusted. Given the difficulties in negotiating international agreements related to cyber war, that subject—though important and appropriate—should probably be handled separately from discussions on the ways in which states could cooperate in enhancing cyber security through the regulation of non-state conduct.

(b). Cyber Intelligence

Even less likely than cyber warfare to become a subject of international agreement is the use of cyber capacities by states for intelligence collection. Intelligence activities have long been and will continue

[45]Convention on International Civil Aviation, December 7, 1944.

to be conducted or sponsored by states subject only to national constraints. Informal understandings designed to avoid damaging cyber (or other) infrastructure may be possible between intelligence agencies of states, especially allies. But such understandings—or other agreements addressed to intelligence collection—are unlikely subjects of multilateral negotiations.

A different problem is posed by efforts of non-state actors to intrude upon and collect intelligence from government or private sources. Such intrusions seem an appropriate subject for international discussions. States may be able to fashion common norms and rules to restrict such conduct, at least in specified situations. Most if not all states have laws that prohibit private individuals from attacking other states without government approval. Such conduct appears in fact from the literature on cyber security to be common and troublesome. Efforts to penetrate private companies for commercial purposes may also be a subject that most if not all states will be willing to address, though where such efforts are officially sanctioned they are likely to be off the negotiating agenda.

(c). Content Restrictions

Virtually all proposals related to cyber security include support for some forms of content restrictions. The CEC includes agreements to prohibit messages that violate copyright laws, hate speech, and child pornography. The SOC acknowledges the right of Member States to prohibit messages that threaten political stability.

The parties to any multilateral negotiation should focus their efforts on securing agreement regarding its most important objectives. If the most important objective of a cyber security treaty is to protect the cyber infrastructure so it can perform its many essential functions, states should focus on protecting against cyberattacks and criminal exploitation that is damaging to ICTs. Negotiators should especially avoid efforts to pursue controversial restrictions of the content of cyber messages that jeopardize agreement on security-related issues. States whose participation in an international cyber regime would be indispensable have significant policy differences concerning the use of cyber networks for political and other forms of expression, and on the relationship of such efforts to national security. While the U.S. properly urges states to agree to allow unrestricted exchanges of ideas and political views,[46] convincing states such as China to alter their policies concerning freedom of communication seems unlikely for the foreseeable future. "A single answer to these . . . questions would leave the world divided and discontented. Decentralized answers to these questions help us get along."[47]

On the other hand, agreement to some content restrictions may be necessary to achieve agreement on cyber infrastructure protection. In such situations, it may be possible to separate such restrictions from infrastructure-protection provisions in order to allow parties to opt into or out of content requirements. At a minimum, the U.S. must insist on retaining the right to refuse to cooperate with political-speech restrictions. The Stanford Draft proposed no content restriction other than "narrow coverage of conduct described as the 'distribution of devices or programs intended for the purpose of committing' other conduct made criminal by the . . ." cyber treaty involved. This provision would permit "safe harbor" sites for discussions of computer vulnerability.[48]

(d). Privacy and Human Rights Limitations

Profound differences exist among potential member states to a cyber security agreement on the privacy and human rights to be accorded users. The U.S. and other democratic societies are justifiably concerned that cyber system regulation—and indeed some measures that strengthen cyber security—may

[46]Secretary of State Hillary Clinton, "Remarks on Internet Freedom" (speech, Newseum, Washington, D.C., January 21, 2010).
[47]"Who Controls the Internet? A Conversation with Jack Goldsmith," Defining Ideas, No. 1 (Stanford University: Hoover Institution, 2010), 100.
[48]Stanford Draft, 9.

also result in reducing the privacy and human rights of users. These concerns will surely compound the difficulties in reaching agreements to enhance security by limiting anonymity.

The ITU Constitution implicitly allows Member States to determine the scope of privacy and other human rights to the extent they are considered matters of domestic security.[49] Expressly recognizing such authority over cyber activities should be avoided, though with the realization that states will still have the power to regulate within their territories. Consensus should be possible, in fact, on including in any cyber-security agreement a reference to widely approved UN conventions bearing upon privacy and human rights, which may in the long run prove helpful in achieving progress on such issues. The Stanford Draft proposed making clear that member states would have no duty "to act in any manner that might infringe upon the privacy or other human rights of any individual or entity, as defined by the law of that State."[50] It proposed establishing within any international cyber-security entity created by agreement a committee of experts tasked with following and reporting on the protection of privacy and human rights, to serve as a forum for ongoing exposure and debate. It also proposed allowing any member state to refuse to cooperate with investigations and prosecutions it considered unfair or inconsistent with its national policies.

(e). National Security Exception

Transnational arrangements often raise issues regarded by states as potentially prejudicial to their national security. Treaties bearing on important national interests often exclude matters considered by any party to threaten its fundamental national security interests. Article XXI of the General Agreement on Trade and Tariffs ("GATT"), for example, states that nothing in the agreement "shall be construed to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security interests," thereby exempting that activity from the regime's rules.[51] The WTO regime has operated effectively in a contentious area, despite its national-interests exception, perhaps because states have exercised that right with restraint, knowing that it is available equally to all parties and that its expansive exercise would deprive them all of the benefits of a regime that serves their interests.

Such situations are especially likely to arise in connection with the creation of cyber norms and standards. For example, sharing information is a fundamental characteristic and benefit of transnational regimes and would be an important aspect of any cyber-security agreement. A government may occasionally be faced, however, with a situation in which sharing information related to a cyber threat could prejudice its security by, for example, revealing vulnerabilities or defensive plans to a state or non-state actor suspected of supporting cyberattacks. States should be permitted, in their discretion, to invoke a national security exception in all such situations.

2. Measures Potentially Applicable to Covered Activities

After identifying those cyber activities (or aspects of such activities) that are likely subjects for international agreement, states considering such agreements must decide what measures to adopt to advance their agreed objectives. States have used or authorized a wide range of measures in international agreements, including: (a) **declarations** that establish common objectives and norms of conduct to achieve them; (b) **information sharing** to provide warnings of dangers and remedies to assist in dealing with them; (c) **prohibitions and punishment of conduct** which the parties agree to make criminal or impermissible under domestic law; (d) **law enforcement cooperation,** including mutual legal assistance and extradition; (e) **standards and practices** that establish mandatory requirements or recommendations

[49]Constitution of International Telecommunications Union, Chapter IV, Article 34: "Member States also reserve the right to cut off, in accordance with their national law, any other private telecommunications which may appear dangerous to the security of the State or contrary to its laws, to public order or to decency."

[50]Stanford Draft, 17.

[51]Article XXI(b), The General Agreement on Tariffs and Trade, 1947.

for equipment, training, and operational activities; (f) **enforcement measures**; and (g) **capacity building** for states requiring assistance.

(a). Declarations of Policy

International treaty regimes uniformly contain declarations of policy related to the subjects they cover. The Preamble of the Chicago Convention declares, for example, that it was adopted "in order that international civil aviation may be developed in a safe and orderly manner and that international air transport services may be established on the basis of equality of opportunity and operated soundly and economically." The Constitution of the ITU (Art. 1) includes among its purposes to "maintain and extend international cooperation between all Members of the Union for the improvement and rational use of telecommunications of all kinds," "to promote and to offer technical assistance to developing countries in the field of telecommunications," "to promote the development of technical facilities and their most efficient operation," and "to promote the use of telecommunication services with the objective of facilitating peaceful relations." In some areas of transnational activity, states issue such declarations without adopting significant, additional measures. Analogous declarations of policy could readily be crafted to express the purposes of an international cyber-security regime. A paper prepared for the NRC by Steve Lukasik describes some types of declarations that could be issued.[52]

Declarations of policy by a sufficiently widespread and influential group of states that confirm cyber security as a universal objective, and that describe appropriate norms of conduct to facilitate achieving that objective, could be useful in creating a more responsible, security-oriented environment than currently exists. Such declarations are commonly issued at the end of conferences, for example, with no expectation they will be treated as enforceable agreements. Alternatively, declarations could be issued that call for specific actions, or that establish specific arrangements or obligations; in the U.S., such agreements might have to be conveyed by the president to the Congress or ratified by the Senate.

(b). Information Sharing

A common feature of international agreements is a commitment to share information considered useful or essential by the parties. Usually, information sharing is only one aspect of a regulatory regime. For example, if a party to the Chicago Convention fails to implement a standard or practice issued with regard to civil aviation, it must under Article 38 "give immediate notification to" ICAO of the differences of its rules from those adopted by the agency. Some agreements are essentially limited to sharing information. In 1986, following the Chernobyl nuclear plant accident, the Convention on Early Notification of Nuclear Accidents required parties to notify each other and the International Atomic Energy Agency of nuclear accidents which have the potential for international transboundary release that could be of radiological safety significance for another state.[53] On December 16, 2000, the U.S. and Russia signed an MOU providing for pre- and post-launch notification of certain missile launches.[54]

Information sharing is certain to be a significant aspect of any international agreement that seeks to enhance cyber security. Parties could agree to share information about attacks or criminal activity; about software and hardware flaws they discover; about methods for increasing the security of computer operations or transactions; and of estimates of losses and damages caused by cyberattacks and exploitation. Efforts could be made on an international basis to overcome the reluctance of companies and individuals to reveal attacks, which typically delay the implementation of effective remedies.

[52]Steve Lukasik, "A Framework for Thinking About Cyber Conflict and Cyber Deterrence," this volume.

[53]"Convention on Early Notification of a Nuclear Accident," September 26, 1986, *Treaty Series: Treaties and International Agreements Registered or Filed or Recorded with the Secretariat of the United Nations* 1439, no. 24404.

[54]"Memorandum of Understanding on Notifications of Missile Launches," December 16, 2000.

(c). Prohibition and Punishment of Specified Conduct

Many international agreements identify types of conduct that parties agree to prohibit and punish. The Montreal Convention, for example, contains a commitment by all Member States to make criminal any form of aircraft hijacking, and to impose severe punishments on persons convicted of such acts.[55] The CEC is modeled on such agreements in that its parties commit to making criminal the forms of cyberattacks and exploitation specified. The ITU GCA identifies types of conduct that many states have agreed should be prohibited, especially attacks on cyber infrastructure, as well as forms of cyber exploitation, such as fraud and theft. States could agree to prohibit these and other activities, and add commitments to prohibit violations of copyright laws, "hate" speech, and other content restrictions. Limits on content have little if any relationship to enhancing cyber security, but their inclusion may be necessary to obtain consensus on security-related provisions.

(d). Law Enforcement Cooperation

Thousands of international agreements, bilateral and multilateral, provide for various forms of law enforcement cooperation. The CEC follows the traditional pattern, and it includes detailed provisions on the collection and preservation of evidence to be used in cyber-related prosecutions. Expanding the CEC regime to additional states and to additional forms of harmful conduct would enhance its effectiveness. This may only be possible, however, if CEC parties agree to join a regime formulated with the participation of non-European states whose support is critical to the successful prevention of cyberattacks and exploitation, and with their concerns in mind.[56] It may also be appropriate (and useful in securing consensus) to exclude from any agreement to prohibit certain types of conduct those interceptions and other activities that do no injury to cyber infrastructure and stem from the failure of users to exercise reasonable care.

As in most treaties calling for the extradition of alleged violators of specified laws of one party found in the territory of another party, member states of a cyber-security regime should be permitted to prosecute alleged violators rather than being required to extradite them. This authority enables a party to ensure that prohibited conduct is prosecuted without sending the individual involved to a state that might fail to provide a sufficiently high level of due process, that might impose unacceptably severe punishment, or for any other reason. In addition, each state could retain the right to treat alleged criminal behavior as immune from prosecution as political offenses or because non-prosecution is required by its national interests. For example, although virtually all states agreed to prohibit aircraft hijacking in treaties to protect civilian aviation, the U.S. and other parties have at times been unwilling to extradite or sometimes even to prosecute individuals for such a serious crime where, for example, the hijacking was done to escape unjust punishment by an oppressive regime. Some states will presumably be even less willing to cooperate in an international regime that strengthens the ability of undemocratic governments to prevent and punish political speech or otherwise restrict or deny fundamental human rights.

A particularly interesting law-enforcement issue is whether states should agree to permit other parties to engage in limited, unilateral actions within their territories to prevent or investigate cyberattacks or crimes in specified circumstances. The CEC's effectiveness has been undermined by its failure to extend this authority, since cyberattacks come suddenly and evidence required to prove who did them is soon lost. Without effective cooperation in preventing and prosecuting cyberattacks and crimes, states and non-state actors are likely to consider engaging in unauthorized and unilateral measures of self-defense, or conducting transnational investigations. The Stanford Draft considered such actions lawful only when based on "legally recognized authority," and acknowledged that "such efforts may affect

[55]Convention for the Unification of Certain Rules for International Carriage by Air," May 28, 1999, *Treaty Series: Treaties and International Agreements Registered or Filed with the Secretariat of the United Nations* 2242, no. 39917.

[56]The Stanford Draft (7), based on a review of then current statutory law, proposed including a commitment by parties to prosecute cyber-related violations of widely approved anti-terrorism treaties.

innocent third parties [even when they] may be reasonable."[57] (A separate paper on such "hackback" or investigative activities has been prepared for the NRC committee).[58]

It would be desirable for parties to a cyber-security agreement to allow limited, specified forms of intrusion of their "cyber space" for information collection and in self-defense, with prompt notification requirements. This authority could be exercised by international teams subject to oversight by all parties in order to avoid the danger that states might abuse such authority for the purpose of conducting an attack or intelligence operation. Standards to govern defensive measures could be developed by an international agency, if one is established, to implement cyber security initiatives. Officially sanctioned and regulated defensive actions would be preferable to unregulated efforts more likely to be overbroad, ineffective, and offensive to the state into whose territory such defensive or investigative actions are undertaken.

(e). Standards and Practices

International governmental organizations ("IGOs") established to protect and foster many types of transnational activities have been given authority (in a variety of forms) to establish rules. In ICAO, these are called (Art. 37) standards and recommended practices ("SARPs"), but are given other names at other IGOs, such as "codes" or simply "rules." These "rules" are often intended to enhance security, safety, and efficiency, objectives that states would seek in negotiating any cyber security agreement. ICAO's SARPs, for example, deal with such matters as airworthiness, registration and identification of aircraft, navigational aids, airports, licensing of pilots and engineers, collection and exchange of meteorological information, investigation of accidents, and other matters "concerned with the safety, regularity, and efficiency of air navigations as may from time to time appear appropriate."

The "rules" adopted by IGOs rarely constitute "law" in the sense of enforceable obligations. States sometimes give IGOs law-making powers, but usually for limited and essential purposes. Normally, states grant IGOs authority to establish what they consider appropriate standards and practices to deal with particular issues, but reserve to all parties the option of declining to implement the rules proposed. Since member states of such institutions participate in fashioning and thereafter approving the standards and practices developed, and because of the frequent need to abide by such rules in order to obtain the benefits of access to the territories and cooperation of other member states, it is rare that states actually decline to follow duly approved rules. While rules adopted by specialized agencies are therefore appropriately characterized as "soft law," they are rarely challenged (though sometimes ignored).[59]

Examples of "soft law" rule making by IGOs abound. In civil aviation, ICAO's thirty-five member Council is empowered to adopt SARPs as (non-compulsory) annexes to the Chicago Convention, and these generally become effective within a designated period unless a majority of Member States disapprove. Though not formally binding, these rules are authoritative, being important for the safety and efficiency of civil aviation. The World Meteorological Organization ("WMO") occasionally adopts technical resolutions through its Congress as "decisions" that it calls on all Member States to do their "utmost" to implement. When these decisions relate to the agency's important World Weather Watch program states able to comply with its requirements generally do so. The International Maritime Organization ("IMO") has established numerous requirements related to navigation, safety equipment, and pollution avoidance, generally approved by its Assembly. While the Assembly consists of representa-

[57]Stanford Draft, 8.

[58]Jay Kesan and Carol Mullins Hayes, "Thinking Through Active Defense in Cyberspace," this volume.

[59]Even legally binding rules can prove ineffective. The World Health Organization ("WHO") Health Assembly is, for example, given express authority by its Member States to adopt regulations binding on all parties except those that reject or make reservations to them by a designated time. The Assembly has rarely exercised this authority, and its most significant action—adoption of its Health Regulations intended to prevent the spread of diseases—was legally upheld but ineffective at securing compliance from the states that it unambiguously bound. Frederic L. Kirgis, Jr., "Specialized Law-Making Processes," in *United Nations Legal Order*, ed. Oscar Schachter and Christopher C. Joyner, Vol. 1, (ASIL, Cambridge Press 1995), 132.

tives of all Member States, it operates through Sub-Committees that deal with technical subjects. It has adopted many nonbinding codes, guidelines, or standards that "are prepared with great care by IMO committees," which are generally successful because "many of the individuals who shape them are also heavily involved in implementing them, either as government officials charged with responsibility for shipping or as representatives of shipping interests."[60]

The Internet (and other cyber systems) currently operate without any formal international institution to set standards or practices, the sort of "soft law" established by many international agencies. The Internet is indeed based on standards, but the term as used by network engineers means something quite different from a SARP. The IETF sets the standards that define the technology of the Internet, but these are "interoperability" standards, and are voluntary. No agency is required to mandate the use of these standards; any actor wanting to participate in the Internet must conform in order to be operating in a manner compatible with the standards being applied by other actors. Similarly, network operators meet as members of the North American Network Operators Group ("NANOG") (which operates internationally despite its name), to discuss operational issues and to set informal standards based on interoperability without being convened by an IGO. Other NGOs, such as ETSI and OASIS, discussed above, operate in the same manner.

Interoperability standards of this sort are common in other areas of transnational activity. In maritime operations, for example, the standards that define the shape and fitting on a shipping container are interoperability standards, and there is no need for an international institution to mandate their use; a non-conforming container would not be shippable. On the other hand, many standards in other areas of transnational activity go beyond being interoperability standards, and must be complied with even though they are not essential in order to function. The standard for the display of navigation lights on vessels of different sizes, for example, is a mandatory requirement, approved by an international institution and enforced by states as a standard or practice.

A significant aspect of the inadequate level of security in cyber operations may stem from the limits to what can be achieved using informal organizations with no power even to adopt "soft law" rules. For example, the Internet community has been discussing the migration from IPv4 to IPv6 for years, with only slow progress. The IETF has defined standards to secure the DNS (the Domain Name System Security Extensions or DNSSEC), which currently has inadequate security, but deployment has been slow due to concerns that should have been resolved in a more timely manner. Similarly, the IETF, working with major equipment vendors, has set standards for a more secure inter-region routing protocol (secure BGP), but these have not been deployed. It is possible that the effectiveness of organizations such as the IETF, ICANN, ISO, ETSI, OASIS, and NANOG could beneficially be complemented by some institution empowered to consider and establish a timetable for the implementation of the standards they propose with the greater authority commonly accorded "soft law" rules promulgated by IGOs.

Establishing cyber-security standards through an international governmental regime seems manageable in some areas, such as criminal law enforcement. Rules have been developed under the CEC that provide deadlines for responding to requests, procedures concerning the seizure of data, production orders, expedited presentation, and disclosure.[61] Similarly, standards or practices could be published concerning notification of attacks, including disclosure requirements, without unmanageable controversy. Another subject that might profitably be addressed in or through a cyber security agreement is how and when disclosure should be made of security flaws in programs, hardware, websites, and other

[60]Frederic L. Kirgis, Jr., "Shipping," in *United Nations Legal Order*, vol. 2, ed. Oscar Schachter and Christopher C. Joyner (ASIL, Cambridge Press 1995), 717. 727-28

[61]See "Convention on Cybercrime." For measures taken at the national level, see Chapter I (specifically Section 2 Article 18 for production order, Article 19 for search and seizure). For measures taken regarding international cooperation, see Chapter II (specifically section 1 Article 24 for extradition, Article 27 for provisions regarding mutual assistance requests). Full text is available at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG (accessed July 23, 2010).

CITs. Disclosures currently can create considerable controversy or even lead to criminal prosecution.[62] Established methods that guaranty safe harbors for such revelations, and perhaps appropriate rewards or recognition, could advance security.

Other problems that could be addressed through standards that go beyond interoperability include, for example, the continued use of software programs considered insecure by the public and even by government agencies performing sensitive tasks;[63] creating agreed bases for liability (by identifying best practices, minimum reliability requirements, and other consensus-based measures) for damages caused by inadequate products or performance by ISPs and other providers; proposals for identifying users being considered by private and government bodies; and the various uses of encryption to enhance reliability without revealing identity.

Presumably, any governmental agency established to consider and promulgate cyber-security standards and practices would build on the interoperability standards fashioned by the IETF or other standard creating bodies and already universally deployed. Such an agency could become a vehicle for considering and adopting existing and future IETF and other acceptable standards with a view toward giving them the authority generally associated with standards promulgated by IGOs. If states agreed to a system that authorized a cyber-security agency to set time periods within which an agency recommended standard should be fully debated, modified, and deployed, the current, informal and uncoordinated system could be strengthened.

(f). Enforcement Measures

International agreements often leave the power to enforce their requirements to the states that join the regimes they operate. IGOs are, however, sometimes assigned authority to collect evidence, hold hearings, make determinations, or impose and enforce remedies against offending states for violations of commitments. The very first, modern, multilateral arrangements, adopted to regularize the collection of tariffs, encourage commerce, and reduce pollution in the Rhine River authorized officials to determine whether violations of commitments were taking place, and ultimately to collect and distribute tariffs to the parties in accordance with an agreed formula.[64] A more recent example is ICAO's power to make and issue findings that an airport is insufficiently secure, where "the practical effect of such a declaration would be to close the airport to international use."[65]

A variety of enforcement powers could conceivably be given to entities assigned cyber-security tasks. Among the most common types of enforcement measures would be the usual powers to establish a budget, to allocate financial obligations to parties, and to suspend the voting rights (or right to participate) of parties that fail to pay their shares of the financial burden of the agency's operations. Authority could also be created for determining responsibility for cyberattacks or exploitation and imposing penalties on non-state actors, including monetary damages and the suspension of licenses.

---

[62]An example of a controversial disclosure is discussed in a Wall Street Journal article published on June 14, 2010, "Compute Experts Face Backlash," B6, col. 1, describes how a group collectively called Goatse Security disclosed a flaw in AT&T's website that made iPad owners' email addresses public. Other experts condemned the disclosure, and the FBI reportedly opened an investigation of the incident. Jeff Moss, founder of the Black Hat security conference said: "We've been having this conversation for 15 years," and still not everyone agrees what is "responsible" disclosure.

[63]Experts appear to regard Windows to be relatively insecure, for example, creating widespread vulnerability. Google, Inc., is reported to have recently instructed its personnel that they may not use Windows on the company's non-portable computers. David Gelles and Richard Waters, "Google ditches Windows on security concerns," *Financial Times*, May 31, 2010, http://www.ft.com/cms/s/2/d2f3f04e-6ccf-11df-91c8-00144feab49a.html.

[64]Thomas Bernauer and Peter Moser, "Reducing Pollution of the River Rhine: The Influence of International Cooperation," *The Journal of Environment Development* vol. 5 no. 4 (December 1996): 389-415. Bernauer and Moser find that such international efforts were modestly and indirectly helpful, and that informal solutions were more effective than formal arrangements.

[65]See Frederic L. Kirgis, Jr., "Aviation," in *United Nations Legal Order*, vol. 2, ed. Oscar Schachter and Christopher C. Joyner (ASIL, Cambridge Press 1995), 853. For more, see the Universal Security Audit Programme (USAP) of ICAO, <http://www2.icao.int/en/ssa/asa/usap/Pages/default.aspx>.

Alternatively, the IGO may be given authority to make determinations, while private actors, such as ISPs, would be relied upon to impose remedies; such private actors will be far more likely to enforce standards against uncooperative users if they are able to rely on approved, international standards or findings to justify enforcement actions.

(g). Capacity Building

Many international regimes include commitments by the parties to provide equipment and training to enable less developed states to acquire the capacities necessary to perform their obligations under the agreement at issue. As a consequence, these states may be able to apply the capacities they acquire to enhance their economic well being. ICAO, for example, together with the United Nations Development Program, engages in many programs each year, involving 80 or more personnel, to "provide training, technical advice, and help in purchasing necessary equipment" to states unable to perform commitments they are prepared to undertake by joining the treaty regime.[66] The ITU has established and is implementing a program to develop cyber security capacities in several states, consistent with its announced, global strategy.

Major programs to assist less developed states develop cyber capacities, including security know-how, are needed in many places. Current efforts along these lines by the U.S. and some other states are limited, and leave many governments incapable of assisting in any cyber investigation or preventive or remedial actions that may be required within their territories. The 2009 Cyberspace Policy Review recommends that the U.S. "should increase resources and attention dedicated to conducting outreach and building foreign capacity. For example, the United States should accelerate efforts to help other countries build legal frameworks and capacity to fight cybercrime and continue efforts to promote cybersecurity practices and standards."[67] Providing this assistance through an international organization would encourage less developed states to join the treaty regime, thereby advancing the objective of creating a uniform and effective set of agreed and binding commitments.

3. Administrative Structure and Powers

The third set of issues that must be addressed in fashioning international agreements regarding transnational activities, including cyber security, are the administrative arrangements and allocations of authority to perform the functions agreed. If the parties to an arrangement agree only on issuing declarations of policy, no administrative structure would be required. The more complex and substantive the functions to be performed on the international level, the more pivotal the process of establishing an effective administrative structure with appropriate allocations of authority. Crafting a suitable structure for an international institution would be critical to its success. To the extent the outcomes desired are rules that are to be adopted as regulations in member states, some sort of governmental approval process will be required. Parties may be prepared to have certain functions performed internationally with one set of administrative arrangements but not with another.

Most IGOs that consider and promulgate rules tend to be structured along established patterns. Several have two representative bodies: a plenary body in which all member states are represented and which usually grants ultimate approval of major decisions; and a smaller, governing body of restricted membership that decides what projects to undertake and manages the process. The technical work of IGOs is often performed by committees of experts that fashion proposals for the IGO's consideration. A Secretariat performs the administrative services required. Voting within the bodies of IGOs varies both as to the body involved, and sometimes as to the issues being determined.[68]

[66]Stanford Draft, 15.

[67]2009 Cyberspace Policy Review, 21.

[68]See generally, Paul Szasz, "General Law-Making Processes," in *United Nations Legal Order*, vol. 1, ed. Oscar Schachter and Christopher C. Joyner (ASIL, Cambridge Press 1995), 48-58.

In fashioning an IGO, or a new assignment for an existing IGO, the treaty-making states are free to specify arrangements that suit their objectives. Important differences exist among IGOs, by design, with regard to the allocation of power to make and approve proposals. A variety of voting arrangements exist, even within the same type of representative body, depending on whether the issue involved is a matter of internal IGO administration (such as its budget), or a matter of external concern.

The potential differences in allocations of responsibilities and authority are especially significant in considering the possibility of international regulation of cyber systems in at least the following respects: (a) whether the current system of **private, professional control over cyber security standards** could continue in its essential composition and methodology; (b) how to ensure **speed and flexibility** in responding to security problems; and (c) what **allocation of powers** to establish among member states regarding agency proposals and internal agency operations.

(a). Maintaining Private, Professional Control over Cyber Security Standards

Perhaps the most fundamental of all issues in considering whether to support international agreements that allocate significant functions related to cyber systems to an IGO is who would participate in developing and approving standards, and how the IGO would relate to existing organizations such as the IETF, ETSI, and ICANN. The current, dominant role of private individuals, entities, and companies in creating, managing, developing, and defending the cyber infrastructure is one of its defining features. The creation of an IGO need not—and in our view should not—entail a shift in the power to perform those functions from the private, volunteer and professional entities and forces that currently dominate cyber standard-setting, to international appointees who may lack the expertise and commitment that private groups have provided since the Internet was created. Such a shift would generate tremendous resistance, since it might place control of standard setting in persons with particular political allegiances inconsistent with universal access and technological progress. Great expertise has been developed regarding cyber threats and security, moreover, within existing private-sector entities, and the support and involvement of these experts would improve the prospect that policies and rules proposed internationally will reflect industry needs and professional opinion rather than political objectives and professionally inadequate conclusions.

Instead of a shift in power, the assignment to an IGO of authority over cyber-security issues could (and should) be fashioned so that it creates a complementary source of power to existing arrangements. An international treaty establishing a specialized agency to regulate cyber security can be fashioned in a manner that preserves private sector influence over the development of cyber system rules. Many multilateral treaty regimes convey substantial influence—amounting in some instances to effective control of key issues—to private sector representatives or entities. The established method for dealing with subject matter that requires "a great deal of technical knowledge" is to grant authority to committees of private-sector experts to fashion technical standards.[69] In ICAO, for example, the 33 member Council is empowered to adopt standards and practices, but these standards and practices must first be considered and recommended to the Council by the Air Navigation Commission (Chicago Convention, Art. 56), a body of fifteen persons with "suitable qualifications and experience in the science and practice of aeronautics" appointed by the Council from nominees of Member States. The ITU operates similarly "with heavy reliance on private-sector expertise and involvement,"[70] though its current internal structure provides no guaranty of professional control over the content of the standards the technical committees propose.

The current standard-setting processes for the cyber world could be incorporated with necessary modifications into an international legal regime assigned this responsibility. Entities such as the IETF, ETSI, OASIS, and ICANN could, for example, be made into or treated as technical committees whose approval of proposed standards is required as a prerequisite to their adoption. This change could not only preserve

[69]Szasz, 53.
[70]Stanford Draft, 14-15.

the current advantages of a private, professional standard-setting regime, it could also, as explained above, enhance its effectiveness. That current privately developed standards are voluntary serves important interests; but in cases related to security and the migration of the core infrastructure to new standards, such as IPv6, an international agency empowered to review, approve, and establish a process for deploying proposed standards could be a useful complement to existing, expert standard-crafting bodies.

Considerable competition has developed in recent years, however, over which agency or agencies will be designated or formed to perform the leading roles associated with a cyber-security regime. The ITU in particular, as noted above, regards itself as having been invested with the role of sole facilitator on cyber security, a role it interprets expansively to include every major function likely to be performed in such a process. The U.S. and other potential parties to an international cyber-security agreement would have to weigh the ITU's possible advantages (existing, experienced, expert, non-duplication of functions, representative) and disadvantages (bureaucratic, political, unwieldy, inefficient, one state-one vote system, lack of guaranteed professional control over standards) in considering its potential cyber-security roles. The ITU and its supporters have not, however, been waiting for the U.S. or any other particular state to make up its mind on how to structure an international cyber-security regime. It will be difficult at this point, therefore, to find a formula for protecting established, privately dominated processes that work well, within a new regime that is essentially governmental and in danger of being subject to politically driven influences.

One significant development over the last several years lends support to the possible preservation of authority for standard setting in private and professional hands. While the Internet Society, the IETF, and ICANN were quite naturally originally dominated by U.S. members and influence, they have become increasingly international entities. Further changes to advance this process without compromising high-quality outcomes could be negotiated, including conceivably the reallocation of "control" the U.S. government has claimed but does not exercise over the authoritative "root" server for domain names and numbering.[71] In addition, highly competent and effective, non-US international standard-setting bodies have become established and represent broad segments of the private sector while also including government participants. Treating these entities as the expert committees on which an agency such as the ITU would be committed to depend could provide a basis for preserving current advantages while expanding the role of other states to an extent consistent with analogous regimes. While the one-state, one-vote formula could be retained for existing functions of an organization such as the ITU, for example, other voting rules could be devised for the IGO's new functions, such as an alternative voting formula for the approval of "soft law" rules, with the usual opt-out option. The possible arrangements that could be developed can only be known through an actual negotiating effort, and further delay in undertaking one is likely to narrow remaining options.[72]

(b). Speed and Flexibility

States can, in fashioning an international agreement, take into account the special needs and characteristics of the activities to be affected. Most specialized agencies of the UN proceed with their work at a slow pace. In some areas, however, speed is essential, and deadlines must be met for the activity to achieve its

[71]Goldsmith and Wu treat the "root" server issue as fundamental. See discussion in Who Controls the Internet, pp. 170-72. The U.S. has responded to complaints on this issue from the EU by establishing the Internet Governance Forum in which states debate and recommend Internet policy issues; it should, if necessary, also consider arrangements that would enable it to share with other states its largely theoretical "ultimate" authority over the process in such a manner that enables it to prevent changes that are unacceptable, as is the case with regard to substantive matters considered by the Security Council.

[72]Opposition is intense to any negotiation that might result in the U.S. agreeing to an ITU role in cyber security. A recent article by Robert M. McDowell, a Commissioner of the Federal Communications Commission condemns the FCC proposal to regulate broadband Internet access services under laws written for "monopoly phone companies" as opening the door to ITU ambitions to regulate the Web. He states: "The best way to keep the Internet open, operating and growing is to maintain the current model." Yet, he also acknowledges that international support for ITU jurisdiction over at least parts of the Internet may be beyond the power of the U.S. to prevent, since "Unlike at the U.N. Security Council, the U.S. has no veto power at the ITU . . . ." Wall St. J., July 23, 2010, p. A17.

intended purpose. For example, information about the discovery of a dangerous infection in a particular area must be conveyed and utilized by health authorities there and throughout the world as quickly as possible, and WHO requirements call for the immediate transfer of such information.[73] A threat to an aircraft in international air space must be dealt with quickly enough to prevent it from being realized.

Care is also taken by some IGOs to ensure that international rules or other actions establish objectives rather than specify the means for achieving them. ICAO, for example, does not require that every party use the same type of equipment to track aircraft or perform some other agreed function; it requires only that each party adopt some method that enables it to perform its agreed function in a satisfactory manner. Similarly, the IMO requires vessels to be able to perform certain activities; it does not normally mandate the purchase of specified equipment or insist upon a particular technology for satisfying those purposes.[74]

Preserving the already limited ability of states to act swiftly and flexibly is particularly important in the cyber security area. The cyber sector is dynamic, with changes that often are faster than expected and impossible to predict. National planners should, if possible, use any international arrangements they negotiate to improve response times to attacks and other threats, perhaps by establishing separate units of politically unaffiliated experts assigned to deal with emergencies. Cyber threats, and their potential defenses, also evolve in ways that are impossible fully to anticipate, and measures adopted to deal with threats sometimes have adverse consequences requiring adjustments. To deal with this problem, international cyber security norms and standards established by declaration, by treaty, or through rules, should be expressed in terms of the results sought, rather than as mandating the use of specific technologies or procedures. The ITU is aware of this potential problem, and has indicated that its proposals will avoid rigid requirements likely soon to be outdated. Preserving the current, private sector control mechanisms for cyber security would help to ensure that these objectives are achieved.

(c). Allocation of Powers

The allocation of powers generally adopted for IGOs could be an appropriate starting point for negotiators in fashioning an entity to perform the functions contemplated in a cyber security agreement. If, for example, the parties agree to continue using the IETF and other private, professional entities as the source of technical cyber security proposals, effective protection would thereby exist against political or technically ill-advised initiatives. Approval of the products of such expert deliberations, by a body backed by governmental authority, on the other hand, is an entirely appropriate political prerequisite for such initiatives to obtain the degree of legal authority agreed upon by the parties. (Some protective mechanism may be required to prevent modifications by the representative entities that do not meet the approval of the technical committee that develops them.) Paul Szasz explained why this mix of power allocation may be optimal:

> The object here is to make certain that any instruments developed will be both technically correct and politically tolerable. This combination may be attained by assigning the task of formulation to a carefully composed expert organ, and having the latter's work vetoed [i.e., reviewed] by a strictly representative one, which may lack technical competence but can make sure that procedures followed at the expert level were satisfactory. These experts would also ensure that there are no major subjective obstacles for any significant state or group of states in the proposed norms.[75]

If it is impossible satisfactorily to integrate existing, private standard-setting bodies into a system within an IGO, it may be preferable to maintain their separate status, counting on their expertise and

[73]World Health Assembly, "Global health security: epidemic alert and response," Resolution WHA54.14, Fifty Fourth World Health Assembly, May 21, 2001.

[74]See Key Principles of IMO's Technical Co-Operation Programme in "IMO and Technical Co-Operation in the 2000s," *IMO Resolution A.901(21),* November 25, 1999.

[75]Szasz, 95.

influence with users to lead the agency to utilize and integrate the privately created standards into agency approved rules and options. In that event, however, the IGO with its separate, expert committees, bureaucratic ambitions, and likely political agenda, could resist privately developed proposals in favor of its own priorities, triggering competitive actions that become an obstacle to continued, technical progress.

V. DIFFICULTIES IN NEGOTIATING INTERNATIONAL AGREEMENTS

Any effort to secure a formal international agreement inevitably entails difficulties and costs, some predictable but others impossible to anticipate. Agreements that are declarations of policy and include no formal commitments pose few problems. But the more formal and inclusive the agreement sought, the greater the uncertainties. Informal declarations of policy may be useful in some situations. But formal and universal commitments are sometimes essential for an agreement to achieve its purposes. Formal commitments to prohibit and punish cyberattacks, to cooperate in prosecuting attackers and criminals, and to adopt agreed measures to enhance safety, would hold more promise of real results than mere verbal pronouncements.

Though more valuable than informal declarations, multilateral agreements providing universal coverage are difficult and time consuming to negotiate, and ultimately provide no assurance that all signatories will abide by their commitments. Conventions related to air and sea terrorism, genocide, and torture have obtained virtually universal agreement from states, but even these fundamental obligations are sometimes violated by parties and high ranking officials. Such agreements are nonetheless made, with full awareness of their imperfections, because of their expected benefits.

The process of securing international agreement on the many controversial issues associated with cyber security is certain to be complex, with uncertain outcomes on some possibly critical issues. Multilateral efforts that the U.S. originally supported concerning climate change, land mines, and an international criminal court resulted in treaties that the U.S. has refused to ratify. Other states have been unwilling to join agreements that the U.S. finds acceptable, notably the CEC. Efforts to extend the reach of a multilateral cyber security agreement to areas of activity where no true international consensus exists seem especially likely to do more harm than good.

The potential costs and uncertainties in securing international agreements, and particularly of utilizing UN mechanisms, can be limited through procedural measures and careful planning. Bilateral and informal arrangements could be used to build toward a broader set of understandings sufficient to justify attempting to create a more conventional, multilateral agreement. Preparatory work with key states should enable participants to identify areas of activity related to cyber security that should be excluded from the negotiating process for reasons identified in this paper, or put on a separate track. Methodical consideration should be given to each type of measure that could be helpful in the development of a more secure cyber infrastructure, keeping in mind that it is unrealistic to identify specific solutions to problems during the negotiating process and that such efforts must be left to the entities the parties agree should be entrusted to implement their policies. The willingness of states—and especially of the U.S.—to accept any significant degree of international, governmental control over cyber security standards and practices will depend on the administrative structures established to exercise the authority conferred.

VI. CONCLUSION

Increased interest in resorting to international cooperation and agreements to enhance cyber security presents a potentially useful opportunity if it is carefully considered and exploited. The areas of cyber activity over which international agreements are most likely to contribute to cyber security must be identified, and they are necessarily those subjects on which the U.S. and other states are prepared to adopt objectives and policies applicable to their own conduct. Cyber warfare (with important exceptions based on existing international law norms), cyber intelligence collection, and content regulation

or standard setting that restrict political speech or limit privacy or human rights, are subjects on which states have conflicting interests, objectives, and policies. On the other hand, cyber infrastructure security seems an area in which all states have strong and consistent interests that they may be prepared to advance through international cooperation and agreements.

Competition over which groups should control the Internet and other cyber systems has long existed. A former battleground for influence was between private groups and the U.S. government, "where over time a form of technocratic self-governance has emerged under the ultimate guarantees provided by the U.S. government."[76] A new and more challenging competition has emerged, however, as states and IGOs seek to establish roles for themselves in a process that Goldsmith and Wu have called "the beginning of a technological version of the cold war, with each side pushing its own vision of the Internet's future."[77] The competition will be resolved either through negotiation or through various forms of conflict likely to be costly and with uncertain results.

In our view, the potential of cyber systems will be most effectively realized by continuing to enable—and indeed enhancing the authority of—an essentially international, diverse, specialized, private and professional set of entities over the technical aspects of the Internet and other, publicly utilized systems. This outcome may, in fact, be more likely through international negotiation and agreement than by continuing a policy of shunning such engagement and allowing the growing competition over power to continue. In the process, the U.S. and other states could enhance security in several areas of cyber activities by authorizing an IGO to perform the many, useful roles such institutions have performed in other areas of transnational activities, while providing governmental backing for rules proposed by the private, professional groups that have made this area of transnational activity so economically productive and socially transformative.

[76]Goldsmith & Wu, 182.
[77]Id. 184.