U.S. International Policy for Cybersecurity: Five Issues That Won't Go Away

Jeffrey Hunker*

On May 29, 2009, President Obama released his Cyberspace Policy Review (the Review).[1] The Review, conducted by the National Security Council and the Homeland Security Council, examined existing government initiatives addressing cyberspace security in order to develop a strategic framework to coordinate government action.[2] The Review put cybersecurity on the policy agenda early in the Obama administration, and it explicitly describes cybersecurity as a global issue that calls for international cooperation:

> The United States . . . needs a strategy for cybersecurity designed to shape the international environment and bring like-minded nations together on a host of issues. . . . Only by working with international partners can the United States best address these challenges, enhance cybersecurity, and reap the full benefits of the digital age.[3]

To date, international aspects have been among the least developed elements of U.S. policy for cybersecurity.[4] The Review lays out some general guidelines for remedying the situation, but it is brief and vague regarding details. This article aims to begin to fill in some of these blanks by exploring in depth the following five issues that demand special attention from the United States and its allies:

1. Improve the Governance Structure for the Internet.
2. Build Norms for Cyber Behavior by Nations and Individual Users.
3. Expand Multilateral Cooperation Against Cyber Crime.

* Currently of Jeffrey Hunker Associates LLC, hunker@jeffreyhunker.com. The author served as Senior Director for Critical Infrastructure, National Security Council, from 1999-2001, and as Director, Critical Infrastructure Assurance Office, U.S. Department of Commerce, from 1998-1999.

[1] CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[2] As used in the Review, "cyberspace" describes the information and telecommunications infrastructure.

[3] CYBERSPACE POLICY REVIEW, *supra* note 1, at iv.

[4] CENTER FOR STRATEGIC AND INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY 69 (2008) [hereinafter CSIS Report], *available at* http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

4. Outline an Evolutionary Path Toward a "New" Internet (Or Alternative Internets).

5. Define the Justification for and Forms of Military Action for Cyberspace.

For each of the above issues, the United States will need to define clear objectives and develop action plans.

In this article, I begin by summarizing what the Review does, in fact, say about the international arena. I then discuss each of the above five issues. In two closing sections, I point out that, while multilateral cooperation is needed to secure cyberspace, there are useful steps that the U.S. government can take unilaterally. I also compare cybersecurity to two other global problems that the international community has managed fairly well – nuclear arms control and chemical weapons control – and identify some lessons that might be learned from efforts in these areas.

I. WHAT THE REVIEW SAYS

Except as noted below, the Review provides little detail concerning the international dimension of U.S. cybersecurity policy. It establishes four principles that form the foundation for an American international agenda. The first principle is that "leadership should be elevated and strongly anchored within the White House."[5] The second principle set out is that the U.S. government will work with the private sector to expand international partnerships and, by implication, help to shape the specifics of U.S. international policy. Third, the Review establishes that the United States will leverage joint interests shared with other countries to drive common policy objectives. That cooperation will include establishing norms for behavior. A fourth principle, mentioned throughout the Review, is that the U.S. international agenda must support free speech and privacy protections.[6]

The Review recommends the following six actions pertinent to international policy:

- Proactively engage international standards bodies working with the private sector. The Review observes, however, that given the multiplicity of international standards bodies – there are more than a dozen active in cybersecurity – many governments will find that such efforts strain their capacities.
- Coordinate with allies on both strategies and operations of network management in order to ensure the stability, interoperability, security, and reliability of the Internet.

[5] CYBERSPACE POLICY REVIEW, *supra* note 1, at iii.

[6] CYBERSPACE POLICY REVIEW, *supra* note 1.

- Document new agreements between governments and industry to enable international information sharing. The Review notes that international collaboration makes government-industry collaboration more challenging.
- Integrate globalization policy with supply chain security to ensure that software and hardware produced overseas do not contain security risks. This topic receives more attention than any other single international issue identified in the Review.
- Support other nations' efforts to build cybersecurity capacity.
- Engage in state-to-state dialogue. The Review lays out some issues that appear to form an agenda for state-to-state dialogue. These include issues that pertain to cyber attack, defense, and deterrence, such as territorial jurisdiction, sovereign responsibility, and the use of force. Other issues relate to cyber crime, including improvements in multilateral cooperation in the investigation and prosecution of cyber crimes.

In fact, when one considers all the action items identified throughout the Review, one finds – not surprisingly, given the global scope of the Internet and the prominence of the United States in shaping that network of networks – that almost all of the Review's action items have international implications. Two such items merit note here and will be discussed later this article. First, the Review recommends that performance and security objectives be identified for the next-generation infrastructure. Second, developing and implementing a successful international agenda will require a large cadre of federal employees with both technical and policy-making skills in cybersecurity. The federal government presently lacks these human resources, and development poses a fundamental challenge to the entire cybersecurity agenda.[7]

I now turn to the five issues, identified above, that should shape the Administration's international agenda. I note external factors that suggest that achieving these goals will not be entirely under the Administration's control.

II. FIVE CRITICAL ISSUES

A. Improve the Governance Structure for the Internet

Whether or not the Internet has a governance structure is a controversial

[7] Interview with Professor David Farber, Carnegie Mellon Univ., former Chief Scientist, Federal Communications Commission, in Pittsburgh, Pa. (July 22, 2009). *See generally* CSIS Report, *supra* note 4, at 72.

subject.[8] Technical protocols for the Internet are adopted by the Internet Engineering Task Force (IETF) through a consensus review of proposals (called Request for Comments, or RFCs). The IETF is not, however, a standard-setting body; adoption of RFCs is voluntary, and there is strong support among some for continuing with the current system.[9] The Internet addressing system is mostly – but not exclusively – overseen by the Internet Corporation for Assigned Names and Numbers (ICANN).

However, there are at least three factors that suggest that the current structure is due for change. First, both the IETF and the ICANN are open to criticism. Under the combined system of the IETF and a host of standard-setting bodies, adoption of security enhancing protocols for the Internet is floundering. Internet Protocol Version 6, which among other features improves Internet security, was approved by the IETF a decade ago, yet the rate of adoption has been extremely low.[10] This is also true for other new security enhancing protocols such as Domain Name System Security Extensions (DNSSEC)[11] and Border Gateway Protocol. That the ICANN is based in the United States and overseen by the U.S. Department of Commerce is a point of controversy.[12] So too is its structure and performance.[13]

A second factor pointing to change is that nations are agitating for a stronger role in – and a more formal definition of – Internet governance. The U.N. sponsored World Summit on the Information Society has considered sweeping reforms of Internet governance.[14] A third reason to anticipate change in the current Internet governance structure is that nations might need to increase their policy and technical cooperation in response to the following developments:

[8] This topic arose at the International Symposium on Global Information Governance held on Sept. 14-15, 2009, in Prague, Czech Republic, *available at* http://www.isgig.org/agenda.shtml. The insufficiency of the mechanisms available to nations for addressing topics such as Internet neutrality, user access, and censorship was a concern discussed at the Symposium, at which I served as chair.

[9] Stephen D. Crocker, *How the Internet Got Its Rules,* N.Y. TIMES, Apr. 7, 2009, at A29.

[10] James Niccolai, *IPv6 Adoption Sluggish: Study,* COMPUTERWORLD, Aug. 25, 2008, *available at* http://computerworld.co.nz/news.nsf/tech/8CF2F74925C98009CC2574AC00750583.

[11] Adoption of DNSSEC has been slow, although the U.S. government mandated federal adoption by December 2009. *See* Kelly Jackson Higgins, *Kaminsky Calls for DNSSEC Adoption*, DARKREADING, Feb. 19, 2009, *available at* http://www.darkreading.com/security/ vulnerabilities/showArticle.jhtml?articleID=21450192 4.

[12] For one side of this controversy, see Phillip Corwin, *Key Members of Congress Call for Permanent ICANN-US Relationship,* INTERNET COMMERCE ASS'N, Aug. 5, 2009, *available at* www.internetcommerce.org/node/201.

[13] *See, e.g.,* Chris Nolan, *ICANN Controversy Is Just the Beginning,* eWeek.com, Nov. 17, 2005, *available at* http://www.eweek.com/c/a/Government-IT/ICANN-Controversy-Is-Just-the-Beginning/.

[14] *See generally* David McGuire, *U.N. Summit To Focus on Internet,* WASH. POST, Dec. 5, 2003, at E05.

- Spread of cyber crime.
- Need for improved attribution of cyber attacks while preserving privacy rights and the occasional need for anonymity.
- Development of next-generation networks to augment or replace the existing Internet.

The roles and structure of the International Telecommunications Union (ITU) offer potentially useful insights. Not all that the ITU does is applicable to the Internet, but it provides some guidance as to how the U.S. government should seek to shift the Internet's governance structure.

The ITU, a U.N. body, is entrusted with harmonizing and coordinating world telecommunications. Like the IETF, the ITU does not "set" standards for phone systems and networks; rather, it "recommends" them, but most if not all ITU recommendations are adopted worldwide.[15] ITU norms rest on four critical elements:

- Universal recognition that standards for international telephony require coordination.
- National systems for translating ITU recommendations into requirements.
- Integration of ITU actions into other agendas, including international trade agreements.[16]
- Recognition of the organizational heft of the ITU itself, based on considerable history.

Further, the ITU has generally done a good job of developing recommendations at or ahead of the curve. For example, the recommendations for a Third Generation (3G) standard were already in place when NTT DoCoMo, a global company at the cutting edge of mobile telephony, began to roll out its multinational strategy for leadership in 3G phones.[17] This situation might be a case of "chicken or egg": the ITU stays

[15] CSIS Report, *supra* note 4, at 8. Legally binding standards can only be set domestically by national standards-setting agencies, such as the American National Standards Institute (ANSI).

[16] In 2001, when China wanted to join the World Trade Organization (WTO), the WTO required that China first commit to ensuring fairly priced and reliable telephone interconnection based on ITU standards. Mattheo Bushehri & Kasra Mottahedeh, *Interconnectivity in China's Telecoms Market,* Asia Case Research Centre, University of Hong Kong, 2006, *available at* http://www.acrc.org.hk/search/case_showdetails.asp?ct=search&c=672&cp=1165&pt=1&pn=1&lv=en.

[17] Ali F. Farhoomand & Vincent Mak, *NTT DoCoMo: Establishing Global 3G Standards,* Asia Case Research Centre, University of Hong Kong, 2003, *available at* http://www.acrc.org.hk/search/case_showdetails.asp?ct=search&c=431&cp=28&pt=1&pn=1&lv=en.

at or ahead of the needs for telephony standards because its requirements play such an important role in how and whether the international telephone system works. The ITU process is sometimes criticized as being slow, but important telephone functionalities have never been unavailable due to ITU inaction.

The Internet is structurally different from the telecommunications system. While the ITU deals with a small number of large corporate or state owned entities, the Internet is run by a multitude of organizations, large and small, and for some of them Internet operations are secondary to other activities. Some ITU practices, such as voting by member states, probably would not work in the IETF. Nor is it clear how the IETF would establish its leverage over Internet providers.

There are large corporate Internet backbone providers and Internet Service Providers (ISPs). As a goal for its international policy, it would be reasonable for the United States to establish ways for these players to cooperate more effectively in implementing protocols that are jointly agreed upon. The ITU offers some guidance as to how Internet security related protocols might be adopted more rapidly by at least the larger players. In this guarded sense, reform to move closer to the ITU model should become a key element of U.S. international cybersecurity policy.

B. Build Norms for Cyber Behavior by Nations and Individual Users

In international policy, norms define expectations for how national governments and their citizens should behave. With well established norms, behavior contrary to a norm often results in national embarrassment or stigmatization.[18] Norms can be informal or codified in specific multinational regimes or treaties.

At present, norms for cybersecurity are only weakly articulated.[19] Establishing norms for cybersecurity needs to take place at two levels – among national governments and, ideally, among individuals. The Council of Europe's Convention on Cybercrime is a promising start for building norms at the level of national governments. But what models might be relevant to individuals?

Consider public health as a model. There is a norm, widely accepted in most countries, that individuals should maintain a certain degree of hygiene – for example, that one must wash hands before eating. There are also norms, appropriate and even socially expected, that require action, such as getting vaccinations. Adherence to such norms is supported by an array of public health bodies at the subnational, national, and international levels.

The U.S. public health system includes over 3,000 county and city health departments and local boards of health, more than 160,000 public

[18] CSIS Report, *supra* note 4, at 21.

[19] *Id.*

and private laboratories, as well as hospitals and volunteer organizations, such as the American Red Cross.[20] At the core is the U.S. Public Health Service, including the Centers for Disease Control and Prevention (CDC), established in 1946. Parts of the system – such as reporting infectious diseases – are voluntary. States are not required to report to the CDC. Nevertheless, the reporting, while not perfect, is good.

Internationally, the World Health Organization acts as a global department of health, overseeing and supervising health activities around the world, as well as undertaking work that can only be done internationally. The structure for public health may appear to be a hodgepodge, and indeed there is room for improvement, but *it works*. For example, smallpox was eliminated worldwide by 1980. Other diseases are being addressed with treatment, prevention, or cures.

Laws, regulations, and inspections mandating health practices are the "big stick" in the public health system; in most jurisdictions children cannot attend school without being vaccinated. The social contract in public health is backed by substantial public investment in water and sewage systems and the like.

Thus, when we call for the development of norms for Internet security, we are not venturing into uncharted territory. It may not be possible or even advisable to replicate what has worked in public health. But this comparison points to the possible need for requirements both proscribing and mandating behaviors on the Internet.

There is reason for hope. Two developments point toward the emergence of new international norms in cybersecurity. One, already discussed, is the Convention on Cybercrime.[21] Expanding the number of countries effectively implementing its provisions provides an important state-sponsored incentive for individuals to comply. It helps to identify those states – and also individual users – that violate its precepts. This is a start.

Another development is the emergence of an institutional infrastructure to support good cyber behavior. The international network of Computer Emergency Response Teams (CERTs)[22] provides a flexible but confederated support system for encouraging good cybersecurity and for responding to security threats in many countries, including the less developed ones. CERTs and other public and private cybersecurity organizations – such as, Information Sharing and Analysis Centers

[20] Sarah A. Lister, *An Overview of the U.S. Public Health System in the Context of Emergency Preparedness* (Cong. Res. Serv. RL31719) (2005), *available at* http://www.fas.org/sgp/crs/homesec/RL31719.pdf.

[21] Convention on Cybercrime, Council of Europe, Nov. 23, 2001, 41 I.L.M. 282, 2296 U.N.T.S. 167, *available at* http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=1&DF=24/02/2010&CL=ENG.

[22] *See* www.cert.org.

(ISACs)[23] and the Internet Storm Center[24] – can be seen as analogs to organizations within the public health structure. CERTs may be said to collect information about the cyber "health" of their regions, assist those "infected," and share this information with other CERTs.

With the harmonization of laws under the Convention on Cybercrime, an international shift toward norms for cybersecurity appears to be a feasible – and an important – goal.

C. Expand Multilateral Cooperation Against Cyber Crime

The lack of effective attribution and the multinational nature of Internet traffic make it difficult to identify and prosecute cyber criminals. Criminal groups can operate in multiple and scattered locations across the globe. National law enforcement agencies cannot investigate most cyber crimes without either investigative support from their foreign counterparts, or the authority to search and seize evidence unilaterally from computers in other countries in pursuit of cyber criminals. Prosecution requires that countries cooperate in locating, holding, or handing over cyber criminals. Thus, multilateral cooperation and authority to conduct cross-border searches are essential elements of effective cyber law enforcement.

Multilateral cooperation against cyber crime operates through informal cooperation and formalized cooperation through the Group of Eight (G-8) industrialized nations and the Council of Europe's Convention on Cybercrime.[25] Informal cooperation is crucial and does not require lengthy treaty processes, but is uncertain. Moreover, extradition of cyber criminals is difficult in the absence of a treaty.[26]

Both the Convention on Cybercrime and the G-8 Subgroup on High-Tech Crime create frameworks for cooperation in investigations between officials in the originating state (of the cyber crime) and those of the target state. The G-8 Subgroup does this unofficially. The Convention on Cybercrime more comprehensively counters cyber crime by harmonizing national legislation, enhancing law enforcement and judicial capabilities, and improving international cooperation. The Convention deems cyber crimes to be extraditable offenses, and permits law enforcement authorities in one country to collect computer-based evidence for those in another. It also calls for establishing a 24-7 contact network to provide immediate assistance for cross-border investigations.[27]

[23] *See, e.g.,* www.isaccouncil.org.

[24] *See* http://isc.sans.org/about.html.

[25] Chris Pounder, *Cyber Crime: The Backdrop to the Council of Europe Convention*, 20 COMPUTERS & SECURITY, 4, 311-315 (2001); Convention on Cybercrime, *supra* note 21.

[26] NATIONAL RESEARCH COUNCIL, CRITICAL INFORMATION INFRASTRUCTURE PROTECTION AND THE LAW: AN OVERVIEW OF KEY ISSUES 42 (Stewart D. Personick & Cynthia A. Patterson eds., 2002).

[27] Kristin Archick, *Cybercrime: The Council of Europe Convention* (Cong. Res. Serv. RS21208) (2008), *available at* http://italy.usembassy.gov/pdf/other/RS21208.pdf.

But so far the United States is the only nation outside of the Council of Europe that has ratified the Convention on Cybercrime.[28] Notable missing parties include China, India, Russia, Canada, as well as other nations of Asia, Africa, and South America. Thus, the Convention does not have the critical mass needed to be effective. Also, there is no effective method for dealing with non-parties – no voluntary understandings with non-party nations, or frameworks for sanctioning countries that are havens for cyber crime.

Expanding multilateral cooperation against cyber crime requires that the United States make progress toward goals in several directions. First, the United States should use its influence to bring about wide and speedy ratification of the Convention. The Convention establishes a legal baseline for effective cyber law enforcement, and the United States should encourage other countries to adopt it, through discussions conducted bilaterally or through regional organizations such as Asia-Pacific Economic Cooperation, the Organization of American States, and the Organization for Economic Co-Operation and Development.[29]

Second, within both the Convention and the G-8 Subgroup, the United States should work to clarify the authority of participating nations to conduct remote cross-border searches (that is, unilateral searches by one nation on computers in another nation for the purpose of seizing evidence). A regime allowing unilateral action is problematic; it is highly unlikely that the United States would ever agree to be at the receiving end of such searches, even if it might like to be on the enforcing side.[30] The United States is more likely to accept a Convention that mandates that ratifying states agree on protocols for authorizing and conducting remote cross-border searches in nations perceived to be havens for cyber crime. Such searches would improve identification of cyber criminals (and arrests of criminals traveling abroad).

Third, as the Review notes, capacity building is important. No nation can be an effective partner in fighting international cyber crime unless it has enacted domestic laws and developed operational expertise to enforce those laws. Nations must also be willing to put these capacities in the service of other countries (victim states or potential victim states).[31] Capacity building in countries lacking these resources is needed.

Sanctions are also important. Any nation that does not ratify the treaty is a potential haven for cyber criminals and cyber terrorists. The United States should develop specific strategies for dealing with countries that are

[28] Convention on Cybercrime, *supra* note 21.

[29] CSIS Report, *supra* note 4, at 22.

[30] For an instance of unilateral cross-border search by the FBI in 2001 see Robert Lemos, *FBI 'Hack' Raises Global Security Concerns,* CNET NEWS, May 1, 2001, http://news.cnet.com/FBI-hack-raises-global-security-concerns/2100-1001_3-256811.html.

[31] CSIS Report, *supra* note 4, at 21.

cyber crime havens. Identifying and sanctioning such nations is an intuitively appealing idea for responding to nation states that pose both cyber crime and cyber war threats.

Such strategies would require that the President work with Congress to define appropriate sanctions and obtain necessary authorities. Sanctions could be very broad – as with the current sanctions on state supporters of terrorism – or narrowly targeted to specific entities, as in the case of the Iran Nonproliferation Act of 2000.[32] Immediate sanctions may turn out to be highly impractical, however. Russia and China have been noted to be havens for cyber crime and non-parties to the Convention.

Another avenue would be to work along the lines of the G-8 Financial Action Task Force (FATF). The FATF comprises countries that have agreed to observe specific best practices for international financial transactions. The FATF's goal is to make money laundering more difficult and more easily detected. The group develops best practices and standards and will not accept new members until they have made progress toward adopting these practices and standards. Members who fail to live up to their obligations face sanctions from the financial community. Prior to 2002, the FATF also had annual evaluations that resulted in some countries being placed on its "Non-Cooperative Countries and Treaties" list (often referred to as the "FATF Blacklist"). While the FATF Blacklist carries no formal sanctions under international law, in practice countries listed on it often found themselves under intense financial pressure. Most large countries with significant financial centers consider transactions involving a country on the FATF Blacklist to be a suspicious activity, triggering greater regulatory scrutiny. This listing appears to have put pressure on blacklisted countries to cooperate in fighting money laundering, but when the list shrank from fifteen to three, it ceased to be updated.[33]

Unlike financial transactions, Internet traffic is mostly free of government oversight. A sanctions regime would require new levels of state cooperation and involvement in Internet management. Though difficult to create, such a regime merits consideration.

Finally, both domestically and multilaterally, the United States should work to improve cooperation. The goal of law enforcement agencies should be to reduce the time required to implement effective cooperation. Even with round-the-clock consultation and mutual assistance processes in place, it is doubtful today that such cooperation will work fast enough to prevent cyber criminals from erasing evidence in some instances.

Likewise, national security organizations should build close collaboration and develop shared policy frameworks reducing response

[32] *Id.*

[33] Amadine Scherrer, *Explaining Compliance with International Commitments To Combat Financial Crimes: The G-8 and the FATF,* paper presented at the 47th Annual Convention of the International Studies Association, San Diego, Mar. 22-25, 2006, *available at* http://www.g7.utoronto.ca/scholar/scherrer.pdf.

times. Network attacks may be deemed intelligence or national security threats and become the responsibility of national security authorities. It might take time to decide whether an event is an act of cyber war, cyber terrorism, or cyber crime. Therefore, one objective of U.S. cybersecurity policy should be to reduce the time necessary to make such determinations. Meanwhile, multiple responses may be necessary – from law enforcement and national security organizations alike.

It is also critical to coordinate these combined responses and then ensure an efficient hand-off to either law enforcement or national security officials when adequate attribution is made. A mature military doctrine can help guide exercise of the various and overlapping legal authorities that apply to cyberspace.[34]

D. Outline an Evolutionary Path Toward a "New" Internet (or Alternative Internets)

The Review states that "performance and security objectives must be defined for the next-generation infrastructure."[35] The existing Internet architecture is fundamentally insecure, and parts of it (such as the domain name system) are very fragile. Many researchers believe that the Internet's shortcomings will not be fixed by conventional, incremental, and "backward compatible" changes in the network. The following are key features of any next generation network:

> The next generation Internet should be secure. It should allow business to set their boundaries and enforce their policies inside their boundaries. It should allow governments to set rules that protect their citizens on the Internet the same way they protect them on other means of transports. It should allow people to set policies for how and where they receive their information. They should have freedom to select their names, IDs and addresses with as little centralized control as possible. The architecture should be general enough to allow different governments to have different rules. . . . The next generation Internet should be designed for mobile objects. . . . The naming, addressing architecture has to allow so that these objects can move and decide how and where they want to receive their Internet traffic with full rights of privacy of their location if desired.[36]

[34] CSIS Report, *supra* note 4, at 24.

[35] CYBERSPACE POLICY REVIEW, *supra* note 1, at v.

[36] Raj Jain, *Internet 3.0: Ten Problems with Current Internet Architecture and Solutions for the Next Generation*, at 1 presented at the IEEE Military Communications Conference (Milcom 2006), Washington, D.C., Oct. 23-25, 2006, *available at* http://www.cse.wustl.edu/~jain/papers/ftp/gina.pdf.

While we cannot be certain that incremental improvements to the current Internet is not the way to go, we do find good reasons supporting the need to start over creating something to replace the Internet.

At present there are a number of research projects worldwide aiming to design and build a "clean slate" Internet. But any such attempt is bedeviled by technical and policy challenges. While it was easy to choose among alternative protocols when the Internet was launched (and indeed there was such a competition),[37] that is not the case now. Besides the technical challenges of designing a new network architecture, we also need a plausible deployment path. What makes this difficult is in no small part the fact that a new, clean slate network will, to a greater or lesser extent, compete with or replace the existing Internet.

The following difficult sets of questions arise when we consider construction of a new infrastructure:

- What do we want to achieve? What is the prioritized list of design criteria for a new system? What elements of the current Internet should be retained?
- Do we want a separate network that serves the special needs of some users, so that we ultimately end up with at least two separate networks (some variant of the current Internet and a new system) or do we want to migrate (sooner or later) from what we have now to something else that completely replaces the Internet? Should the new network be accessible (sooner or later) by everyone, or should it be run on an "invitation only" basis? Choices could, for example, range from a network limited to the U.S. Department of Defense to one open to global adoption, with the current Internet being rapidly phased out.
- Should the new network be backward compatible with the existing Internet? How do existing administrative structures and network economic forces match with potential trajectories for a clean slate network adoption? This question takes on even more relevance because of the ongoing discussion about Internet governance at the World Summit on the Information Society.[38]
- How do we achieve what we want? Who are "we"? What roadmap, including research & development and implementation,

[37] The competition for Internet protocols involved protocols from IBM, Digital Equipment Corporation, and Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP was eventually chosen. *See* Brian M. Leinen, et al., *A Brief History of the Internet*, THE INTERNET SOCIETY, *available at* http://www.isoc.org/internet/ history/brief.shtml.

[38] *See* World Summit on the Information Society, Internet Governance Forum, http://www.itu.int/wsis/implementation/igf/index.html.

> would lead us to our goal? What cornerstone high payoff projects or experiments should be executed in the short term to create the best foundation for our ultimate goal?

The United States must develop a vision of future network alternatives that answers these questions in a way that serves U.S. national interests. Whatever choices are made will have international implications. U.S. policy must also determine what role, if any, the U.S. government will play both domestically and internationally. While much attention is being paid to the technical aspects of Internet alternatives – by, for example, the Global Environment for Network Innovations (GENI) – little attention appears directed to consideration of these questions of U.S. international policy.

E. Define the Justification for and Forms of Military Action for Cyberspace

Conflict waged between nation states in cyberspace is a looming challenge. Arguably, state sponsored cyber attacks already have occurred. Russia has been accused of conducting cyber warfare campaigns against Estonia in 2007, Georgia in 2008, and Kyrgyzstan in 2009.[39] Russia denies any state involvement. Whether that is true or not, the threat of offensive cyber operations will continue to grow in importance.[40] For example, China is developing cyber operations as a tool of warfare, and will likely use this tool in any future conflict with the United States to exploit national dependence on cyberspace.[41]

However, the form and purpose of cyber military action is still evolving. Cyber attacks appear to have been used in the Russia-Georgia conflict to soften up targets in advance of kinetic attack. Alternatively, a "slow" cyber attack might be launched, gradually degrading infrastructures or penetrating information systems over a protracted period of time. Cyber warfare competition is shrouded in secrecy, making it difficult to determine national vulnerabilities and threats – and therefore to gauge whether a purely defensive strategy is appropriate, or whether offensive capabilities are needed to create a credible deterrent.[42]

Defining the justification for and form of military action in cyberspace comprises a complex but urgently needed agenda. The United States is

[39] Andrew F. Krepinevich, Jr., *The Pentagon's Wasting Assets*, FOREIGN AFFAIRS, July/Aug. 2009, at 18, 25.

[40] CSIS Report, *supra* note 4, at 12-14.

[41] U.S.-CHINA ECON. AND SECURITY REV. COMM'N, 2008 ANNUAL REPORT TO CONGRESS 163, 167 (2008), *available at* http://www.uscc.gov/annual_report/2008/annual_report_full_08.pdf.

[42] Krepinevich, *supra* note 39, at 30-31.

already engaged in bilateral discussions concerning military use of cyberspace. Reportedly, Russia supports forging an international treaty banning countries from engaging in cyber war, similar to past chemical warfare negotiations. The United States has advocated improved cooperation among law enforcement agencies. The reasoning is that if cyber criminal institutions and cyber attacks are declared illegal, this will in turn cause military attacks to be deemed illegal.[43]

As other contributors to this journal issue discuss,[44] defining policy for military operations in cyberspace is a daunting challenge: who exactly is attacking us, is a kinetic response to cyber attack justified, and if so, under what circumstances? These questions must be addressed as critical elements of U.S. international cyber policy.

III. Final Considerations

A. *Unilateral Actions That Can Have International Impact*

The United States has many different means to advance its international goals. Most of them involve some direct engagement with other countries or constituencies. But with Internet security, the United States also has the opportunity to advance its agenda by unilaterally leveraging its role in the global Internet. The nation has been a leader in number of users, content developed and shared, the emergence of new applications, and software and hardware developed.

Even state-level unilateral action can have international consequences. To illustrate, New York State's requirement that any fire insurance company operating in the state share its actuarial information (to create a common data set) led, in 1914, to a nationwide data-collection bureau that "enabled the development of modern actuarial science in the fire field."[45]

Unilateral action to achieve international goals can take a number of forms. Four areas to be considered are:

- Procurement: The U.S. government can enforce requirements that only properly configured, secure software, and secure hardware be acquired. These requirements are, in fact, already in place, but they have not been adequately specified or observed in practice.[46]

[43] John Markoff & Andrew E. Kramer, *U.S. and Russia Differ on a Treaty for Cyberspace,* N.Y. TIMES, June 28, 2009, at A1.

[44] *See* Herbert S. Lin, *Offensive Cyber Operations and the Use of Force* 4 J. NAT'L SECURITY L. & POL'Y 63 (2010); David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SECURITY L. & POL'Y 87 (2010).

[45] Dalit Baranoff, *Fire Insurance in the United States*, EH.NET, *available at* http://eh.net/encyclopedia/article/Baranoff.Fire.final.

[46] *See, e.g.*, U.S. GOVERNMENT ACCOUNTABILITY OFFICE, INFORMATION SECURITY: AGENCIES CONTINUE TO REPORT PROGRESS, BUT NEED TO MITIGATE PERSISTENT WEAKNESSES,

- Regulations: I join others who believe that cyberspace cannot be made secure without regulation. Federal government standards for cybersecurity and some critical infrastructures (such as banking and finance) would help set benchmarks or best practices worldwide. I recognize that creating such regulatory structures is fraught with difficulty and challenges, but it is not out of the question.
- Market Access: The President could mandate that federal agencies contract only with telecommunications providers that use secure Internet protocols. Even more proactively, national connectivity with the global Internet might be structured so as to favor nations and providers using secure protocols and practices.
- Liability: Imposing product liability on insecure software would create economic incentives for vendors to do better on quality and security. Producing better software may not now be in the business interests of most software producers. Imposing liability would require either an evolution in how the courts address these matters, or action by Congress and the President to impose liability through legislation.

Each of these forms of unilateral action is highly controversial, and each would require judicious structuring and implementation. Close cooperation with industry will of course be necessary. Implementation would have international as well as domestic consequences, and thus these unilateral actions would be significant elements of U.S. international policy.

The key question, however, is whether the U.S. government will be capable of taking consistent, significant actions to support its international goals. Of the actions enumerated, the only one available currently is government procurement. The Review calls for a mid-term action to "refine government procurement strategies and improve the market incentives for secure and resilient hardware and software products."[47] There is further discussion of other economic instruments (such as liability). Launching federal procurement strategies to improve cybersecurity is not new; however, the history of past efforts[48] does not

NO. GAO-09-546 at 40-41 (2009), *available at* http://www.gao.gov/new.items/d09546.pdf.

[47] CYBERSPACE POLICY REVIEW, *supra* note 1, at 38.

[48] The National Information Assurance Partnership (NIAP) evaluates information security products and requirements for federal procurement to align government purchasing with security standards. Product security standards for procurement have been challenged on a number of issues, including whether secure products, once connected, still comprise a secure system, the time required for evaluation versus the rate of market change, and the adequacy of the testing protocols themselves. For a discussion of a program under the NIAP aimed at evaluating IT product conformance to international standards, called the NIAP

suggest much promise for the future. A new federal policy structure with "leadership from the top," as outlined in the Review, however, might provide the wherewithal to devise and implement meaningful unilateral action in each of these areas.

B. Is the Proposed International Strategy Feasible?

Looking toward existing international regimes that have parallels to cyber seems a useful way of gaining insight into what an international cybersecurity regime might look like. Parallels with nuclear arms control have been drawn in the past, notably a decade ago in the context of the U.S.-Russia dialogue concerning conflicts in cyberspace. The following similarities between the nuclear and cyber threats may be instructive:

- Nuclear and cyber threats are complicated issue areas that involve technology-based dangers that must be controlled globally.
- The management of nuclear and cyber threats requires implementation of measures flexible enough to deal with a range of possible malefactors, including criminal gangs, rogue states, and stateless entities.
- Verification in nuclear arms control is in some respects comparable to the "attribution" issue in cybersecurity.[49]

But there are major differences as well. Nuclear arms control involves a small number of nations that possess nuclear capabilities, and despite the fact that the technologies are over half a century old, the difficulty of acquiring the capability to build nuclear weapons is not a trivial barrier to other nations. The distinction between peaceful uses of nuclear power and the development of nuclear weapons is fairly clear-cut. Verification of compliance with nuclear test ban treaties[50] is straightforward, based on seismic and atmospheric monitoring. Other aspects of verification in

Common Criteria Evaluation and Validation Scheme for IT Security, or CCEVS, see http://www.niap-ccevs.org/aboutus.cfm.

[49] *See* WILLIAM J. PERRY, CHARLES D. FERGUSON & BRENT SCOWCROFT, U.S. NUCLEAR WEAPONS POLICY: INDEP. TASK FORCE REPORT NO. 62 (2009). For further discussion about U.S. nuclear weapons control, see CSIS Report*, supra* note 4, at 16, 20, 43.

[50] *See, e.g.,* Treaty Banning Nuclear Weapons Tests in the Atmosphere, in Outer Space, and Under Water, Aug. 5, 1963, 14 U.S.T. 1313, 480 U.N.T.S. 43; s*ee also* http://www.nti.org/db/China/ptbtorg.htm (providing a summary and information regarding China and the treaty). The Comprehensive Nuclear Test Ban Treaty (not yet in force) would ban underground testing as well. The full text of the treaty is available at http://www.ctbto.org/the-treaty/treaty-text/.

nuclear arms control, such as verification that missiles or warheads have been disarmed, are more complicated but feasible to some extent.[51]

Few of these characteristics describe cyber threats. Building cyber attack tools is mostly a matter of writing software code, a capability which nearly every nation and many individuals have mastered. The same software codes that can in one formulation be used in a cyber attack or penetration frequently also have commercially or socially useful purposes. So called "botnets" harness the power of multiple distributed computers to launch attacks that shut down the Internet for organizations and even countries. The same botnet architecture, however, harnesses the power of thousands of computers whose owners willingly donate some of their computers' calculating power to help perform complex scientific calculations.[52] For these reasons, banning the use of cyber attack tools is a tricky affair.

The Chemical Weapons Convention[53] arguably provides a better model for comparison. The production of chemical weapons is easily within the reach of both nations and subnational groups. Like cyber, many chemical weapons have a dual use. Verifying compliance with any restrictions is difficult at a distance and requires on-site inspections.

The Chemical Weapons Convention was the product of decades of diplomacy. Following the experiences of World War I, international agreements about chemical weapons were first formalized with the 1925 Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or other Gases, and of Bacteriological Methods of Warfare, usually called the Geneva Protocol. This treaty prohibited the use of chemical and biological weapons on the basis that they were indiscriminate in their impact.[54] However, it did not address production, storage or transfer of chemical or biological weapons.

It was not until 1962 that the Eighteen-Nation Committee on Disarmament was formed, and not until 1992 that the text of the Chemical Weapons Convention was presented to the United Nations.[55] The

[51] *See, e.g.*, Andreas Persbo & Marius Bjorningstad, *Verifying Nuclear Disarmament: The Inspector's Agenda*, ARMS CONTROL TODAY, May 2008, *available at* http://www.armscontrol.org/act/2008_05/PersboShea.

[52] One large "scientific botnet" is used in the SETI@home project to search for signs of extraterrestrial intelligence; project data *available at* http://setiathome.berkeley.edu/.

[53] Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, Sept. 3, 1992, S. Treaty Doc. No. 103-21, 32, 1015 U.N.T.S. 163 [hereinafter Chemical Weapons Convention].

[54] Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, June 17, 1925, 26 U.S.T. 571, 94 L.N.T.S. 65.

[55] Chemical Weapons Convention, *supra* note 53; s*ee* Background to the Chemical Weapons Convention, United Nations, *available at* http://www.un.org/Depts/dda/WMD/cwc/. Transcripts of Eighteen-Nation Committee proceedings are *available at* http://quod.lib.umich.edu/e/endc/.

Convention is now ratified by almost all nations, and provides for a commitment for reducing and eliminating (by 2012) all stockpiles of chemical weapons, as well as a framework for on-site inspections and other means of verification.[56]

The Convention categorizes chemicals and their feed stocks based on the extent to which they are used for peaceful purposes. Use of certain agents – tear gas, pepper spray – is specifically allowed in domestic law enforcement. Verification of compliance with requirements to destroy chemical weapons stockpiles, or the facilities for manufacturing these weapons, requires on-site inspections, which are provided for under the Convention.[57] The U.S. government, for instance, proudly announced recently the one hundredth inspection of a U.S. chemical facility under the Convention.[58] For countries suspected of non-compliance, such as Iraq during the 1990s, on-site inspections for chemical weapons became a major focus of international diplomacy.[59]

The Convention is monitored by an independent agency not affiliated with the United Nations, and is in parallel with an accompanying treaty dealing with biological weapons.[60]

Reduction of chemical weapons illustrates that a long term commitment backed by multinational cooperation can provide a workable regime for controlling and eventually eliminating a class of dangerous agents that lie within the ambit of all nations to produce and use. The potential use by subnational groups still exists (witness the Sarin gas attack in Tokyo subways), but to date we have seen only limited threats.

This example of multinational cooperation creating a regime for the control of a threat easily within the reach of any nation or subnational group suggests that cooperation can lead to the creation of a similar regime for cybersecurity. Some lessons that may be drawn from this experience are:

- The development of the Chemical Weapons Convention took decades. A cybersecurity regime might occur much more quickly but will still take time.
- The process involved the creation of new infrastructure (outside of existing institutions such as the United Nations) for monitoring compliance.

[56] Chemical Weapons Convention, *supra* note 53.

[57] *Id.*

[58] U.S. Dep't of Commerce & U.S. Dep't of State, U.S. Chemical Weapons Convention Website, http://www.cwc.gov/.

[59] The United Nations provides a summary of issues related to inspections in Iraq, *available at* http://www.un.org/Depts/unscom/Chronology/chronologyframe.htm.

[60] Chemical Weapons Convention, *supra* note 53.

- The process of totally eliminating the threat by reducing stockpiles is still ongoing; the challenge is to manage this transition.

Chemical weapons control is not a static concern; issues can emerge and mature over time. Witness the inclusion of chemical weapons within the broader problem of weapons of mass destruction (WMDs). As the CSIS report pointed out:

> Twenty years ago, the proliferation of WMD was often an afterthought in discussions of the strategic environment. With the end of the Cold War and the reprioritization of U.S. strategy, the profile of nonproliferation in national security grew rapidly. After 1989, the president created an NSC directorate and issued new policies and directives, and Congress passed legislation providing authorities and sanctions; regulations were published and the Department of State (DOS) and the Department of Defense (DOD), and the intelligence community established offices to deal with the new challenge. Internationally, the United States created new multilateral organizations for coordinated action against WMD, and reenergized existing ones, and made nonproliferation a norm for international behavior and a factor in every major initiative.[61]

The following questions, currently left hanging, deserve careful thought:

- If we cannot afford taking many years to arrive at a mature global regime for cybersecurity (and we arguably cannot), what can we do to accelerate the process? The Review does not specify time frames for international action.
- Can we achieve with attribution what has been achieved with on-site verification in chemical weapons?
- With chemical weapons, U.S. interests can be clearly stated: to protect the security of the United States and its allies by promoting nonproliferation of weapons, a reduction in weapons by those countries possessing them, and measures to ensure that WMD do not get in the hands of terrorists. When, if at all, will it be possible to state U.S. international goals in cybersecurity in a similarly crisp fashion?

We are not likely to solve the problems of cybersecurity any more than we have "solved" the problem of chemical weapons use for all time. Both are situations that need to be *managed.* Still, success to date in dealing with the chemical weapons threat gives hope for cybersecurity.

[61] CSIS Report*, supra* note 4, at 19; *see id.* at 21 ("the WMD precedent is useful").

CONCLUSION

The international agenda for cybersecurity remains one of the least developed parts of U.S. policy. It is refreshing that the Review recognizes the importance of a robust international agenda. The key challenge for the United States is to define clear objectives for its international cybersecurity policy, and develop action plans for achievement. This article has suggested the key areas to focus on in the coming years.