The Past, Present, and Future of Cybersecurity

Walter Gary Sharp, Sr.[*]

> *Are these the shadows of the things that Will be, or are they shadows of things that May be, only? . . . Men's courses will foreshadow certain ends . . . . But if the courses be departed from, the ends will change. Say it is thus with what you show me.*[1]

The cyber threat is the most pervasive and pernicious threat facing the United States today. Its mention does not immediately conjure visions of the catastrophic horrors that would result from an attack using a weapon of mass destruction, but today's cyber threat is a very real and present danger. As of September 14, 2009, more than 10,450,000 U.S. residents had been victimized by identity theft in 2009 alone, and that number increases by one victim each second.[2] Fifteen million victims will lose more than fifty billion dollars each year.[3] Specific threats such as identity and consumer fraud allow us to quantify and understand part of the cyber threat in terms that allow the U.S. government,[4] corporate America,[5] consumer groups, and individuals[6] to take preventive action. However, the growing number of victims would clearly suggest we have not effectively solved the problem, even if we are starting to comprehend its scope.

The cyber threat to U.S. national security, economic security, and public health and safety is far more amorphous and less susceptible of comprehension than its kinetic analogs. Popular media productions such as *24*[7] and *Live Free or Die Hard*[8] have depicted sophisticated cyber intrusions that intentionally caused aircraft collisions, a nuclear power plant meltdown, a compromise of White House security and communications,

[*] Senior Associate Deputy General Counsel for Intelligence, Office of the General Counsel, U.S. Department of Defense; Adjunct Professor of Law, Georgetown University Law Center; and Judge Advocate, U.S. Marine Corps (Retired). Opinions, conclusions, and recommendations expressed or implied herein are solely those of the author and do not necessarily represent the views of the U.S. Department of Defense or any governmental agency or civilian institution.

[1] CHARLES DICKENS, A CHRISTMAS CAROL, at Stave 4(1843), *available at* www.stormfax.com/dickens.htm.

[2] *See 2009 Security Breaches and Database Breaches*, www.identitytheft.info/breaches09.aspx.

[3] *See Identity Theft Victim Statistics*, www.identitytheft. info/victims.aspx.

[4] *See, e.g.*, Fed. Trade Comm'n Identity Theft Website, www.ftc.gov/bcp/edu/microsites/idtheft.

[5] *See, e.g.*, John P. Bonora, *Shadow Wars: Managing an Effective Identity Theft Prevention Program*, ABA BANK COMPLIANCE, Mar.-Apr. 2009, at 8.

[6] *See, e.g.*, www.identitytheft.info.

[7] *See* Fox Broadcasting Company *24* Website, www.fox. com/24.

[8] *See* The Internet Movie Database, *Live Free or Die Hard*, www.imdb.com/title/tt0337978/.

and a U.S. stock market crash. Recognizing the extent of abuse of the Internet for "terrorist purposes, including through radicalization, recruitment, training, operational planning, fundraising and other means," the United Nations established a Working Group on Countering the Use of the Internet for Terrorist Purposes.[9] The Cyberspace Policy Review (the Review) directed by President Obama reports that 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."[10] It is only a matter of time before terrorists attempt to use the Internet to cause acts of terrorism – like those already described in popular media.

I. THE GHOST OF CYBERSECURITY PAST[11]

Executive Order 13,010, *Critical Infrastructure Protection*, publicly declared fourteen years ago that cyber threats exist that could have a "debilitating impact on the defense or economic security of the United States" and that "it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation."[12] This executive order established an intergovernmental body titled the President's Commission on Critical Infrastructure Protection (PCCIP).

The PCCIP was charged with wide ranging mission objectives that entailed an assessment of the threat and vulnerabilities and a recommendation for a "comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats and assuring their continued operations."[13] The PCCIP delivered its 192-page report to the President on October 13, 1997, calling for a national effort to assure the security of the increasingly vulnerable and interconnected infrastructures such as telecommunications, banking and

[9] United Nations Website, *U.N. Action To Counter Terrorism, Working Group on Countering the Use of the Internet for Terrorist Purposes*, http://www.un.org/terrorism/workgroup6.shtml.

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

[11] This section and the next section on more recent cybersecurity initiatives are not intended to identify all past and present U.S. cybersecurity efforts. Rather, they are intended to identify the earliest significant efforts – Executive Order No. 13,010 and Presidential Decision Directive (PDD) 63 – and the present most significant efforts – the Comprehensive National Cybersecurity Initiative (CNCI) and the Department of Homeland Security. See Appendix C of the *Cyberspace Policy Review* for a more detailed description of the development of supporting U.S. legal and regulatory frameworks associated with the growth of modern communications technology.

[12] Exec. Order No. 13,010, *Critical Infrastructure Protection*, 61 Fed. Reg. 37,347 (July 15, 1996).

[13] *Id.* at 37,348.

finance, energy, transportation, and essential government services that constitute the life support systems of the United States.[14]

The PCCIP's extensive work and recommendations culminated in Presidential Decision Directive 63 (PDD 63), which was signed by President Clinton on May 22, 1998.[15] President Clinton's intent was to "take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems."[16]

PDD 63 created a National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, and a Critical Infrastructure Assurance Office to support the National Coordinator's work. It also established a National Infrastructure Protection Center (NIPC) to coordinate information sharing among federal departments, agencies, and the private sector. PDD 63 also set up the National Infrastructure Assurance Council, which includes state and local officials and private operators of critical infrastructure. The Council was to assist in the development of a national Critical Infrastructure Protection plan.[17] PDD 63 also encouraged the private sector to set up Information Sharing and Analysis Centers (ISACs) to facilitate information sharing and coordination.[18]

PDD 63 set the national goal of achieving an initial operating capability no later than 2000 and a full operating capability to protect U.S. critical infrastructures no later than 2003.[19] In January 2000, the Clinton administration published its national plan titled *Defending America's Cyberspace: National Plan for Information Systems Protection, Version*

[14] ROBERT T. MARSH, CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES (1997), *available at* http://chnm.gmu.edu/cipdigitalarchive/files/5_ Critical FoundationsPCCIP.pdf. A number of the reports submitted by government and private sector groups to the PCCIP for use in developing its recommendations are available at the George Mason University Critical Infrastructure Protection digital online archive. Most notable are the twelve *Legal Foundations* reports that contain almost 600 pages of analysis that attempt to identify and describe many of the legal issues associated with the process of infrastructure assurance. The first report is the summary report that describes and summarizes seven discrete legal issue areas: major federal legislation, adequacy of criminal law and procedure (cyber), adequacy of criminal law and procedure (physical), privacy laws and the employer-employee relationship, legal impediments to information sharing, federal government model performance, and approaches to cyber intrusion response.

[15] Presidential Decision Directive 63 [hereinafter PDD 63], *Critical Infrastructure Protection* (May 22, 1998), *available at* http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

[16] *Id.* at §II.

[17] *Id.* at §VI.

[18] *Id.* at Annex A.

[19] *Id.* at §III.

1.0: An Invitation to a Dialogue.[20] Its principal focus was the protection of America's cyberspace through the creation of public-private partnerships.[21]

Although the new Bush administration initially continued the cybersecurity policies of the Clinton administration, the terrorist attacks of September 11, 2001, caused President Bush to shift the principal focus of critical infrastructure protection from cyber attack to physical attack.[22] President Bush signed Executive Order 13,228 on October 8, 2001, establishing an Office of Homeland Security within the Executive Office of the President.[23] Its mission was "to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks."[24]

Congress then created the Department of Homeland Security (DHS) in November 2002.[25] One primary mission included preventing terrorist attacks within the United States and reducing the vulnerability of the United States to terrorism, but the DHS was also assigned significant responsibilities and authorities for information security and the protection of critical infrastructure information.[26]

President Bush signed Homeland Security Presidential Directive 7 (HSPD-7) on December 17, 2003.[27] The purpose of HSPD-7 was to establish a "national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks."[28] HSPD-7 identified the responsibilities of the heads of the federal departments and agencies. It also defined the role of the Secretary of the DHS for "coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States."[29] The Secretary of the DHS was also designated "as the principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, state and local governments, and the private sector to protect critical infrastructure and key resources."[30]

As the next evolution in President Clinton's *National Plan for Information Systems Protection*, President Bush released the *National*

[20] DEFENDING AMERICA'S CYBERSPACE: NATIONAL PLAN FOR INFORMATION SYSTEMS PROTECTION, VERSION 1.0: AN INVITATION TO A DIALOGUE (2000), *available at* www.fas.org/irp/offdocs/pdd/CIP-plan.pdf.

[21] *See id.*

[22] John D. Moteff, *Critical Infrastructures: Background, Policy, and Implementation* (Cong. Res. Serv. RL30153), Oct. 10, 2008, *available at* www.fas.org/sgp/ crs/homesec/RL30153.pdf.

[23] Exec. Order No. 13,228, 66 Fed. Reg. 51,812 (Oct. 8, 2001).

[24] *Id.*at §2.

[25] Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135.

[26] *Id.*

[27] Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection* (Dec. 17, 2003).

[28] *Id.*

[29] *Id.*

[30] *Id.*

Infrastructure Protection Plan (NIPP) on June 20, 2006.[31] Its purpose was to "reduce vulnerability, deter threats, and minimize the consequences of attacks and other incidents."[32] It designated seventeen critical infrastructure and key resource sectors and set a timeline for developing sector-specific plans for each sector.[33] Updated in early 2009 by DHS Secretary Michael Chertoff, the NIPP set forth "focused, risk-informed prevention, protection, and preparedness activities" to protect U.S. critical infrastructure and key resources by "preventing catastrophic loss of life and managing cascading, disruptive impact on the U.S. and global economies across multiple threat scenarios."[34]

II. THE GHOST OF CYBERSECURITY PRESENT

A detailed description of the existing statutory and regulatory framework for cybersecurity is beyond the scope of this article. In brief, that framework assigns responsibility and authority for cybersecurity to the heads of federal departments and agencies. Consider, for example, the Federal Information Security Management Act (FISMA) of 2002.[35] FISMA authorizes the Director of the Office of Management and Budget (OMB) to oversee federal agency information security policies and practices for systems that are not national security systems, but assigns primary responsibility to the heads of federal agencies for providing information security protections for all information and information systems of their respective agencies. Except for the limited oversight of and standards set by the Director of OMB, FISMA does not provide for any true coordination or interoperability among federal departments and agencies. Similarly, PDD 63 provided that "every department and agency of the federal government shall be responsible for protecting its own critical infrastructure, especially its cyber-based systems," but it assigned the National Coordinator the responsibility for coordinating governmental interdependencies.[36]

At the DHS, steps have been taken to develop the role of coordinator of federal cyber security. The DHS states that it "has the lead responsibility for assuring the security, resiliency and reliability of the nation's Information Technology and communications infrastructure *although*

[31] NATIONAL INFRASTRUCTURE PROTECTION PLAN: PARTNERING TO ENHANCE PROTECTION AND RESILIENCY (2009) [hereinafter NIPP]. The updated NIPP, released in 2009, is available at http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

[32] Department of Homeland Security, *NIPP Risk Management Framework*, *available at* http://www.dhs.gov/xlibrary/assets/NIPP_RiskMgmt.pdf.

[33] NIPP, *supra* note 31.

[34] *Id.* at iii.

[35] Federal Information Security Management Act of 2002, 44 U.S.C. §§3541-3549 (2006).

[36] PDD 63, *supra* note 15.

efforts to protect our federal network systems from cyber attacks remain a collaborative, government-wide effort."[37] However, the DHS is a leader in a consensus-based process that allows federal departments and agencies a fairly wide range of independence.

On January 2, 2008, President Bush "approved National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD 54/HSPD 23), which formalized a series of efforts designed to further safeguard federal government systems and reduce potential vulnerabilities, protect against intrusion attempts, and better anticipate future threats."[38] NSPD 54/HSPD 23 established the Comprehensive National Cybersecurity Initiative (CNCI).[39] Under the CNCI, the DHS has the authority to lead national efforts to:

- Establish a frontline defense to reduce current vulnerabilities and prevent intrusions.
- Defend against the full spectrum of threats by using intelligence and strengthening supply chain security.
- Shape the future environment by enhancing our research & development and education, and by investing in leap-ahead technologies.[40]

As an example of one initiative undertaken to accomplish its CNCI responsibilities, the DHS is currently deploying the Einstein Program within the DHS and plans to expand it to all federal departments and agencies.[41] The Einstein Program is an early warning system that will help "identify unusual network traffic patterns and trends which signal unauthorized network traffic so security personnel are able to quickly identify and respond to potential threats."[42]

Executive Order 13,010 and PDD 63 established the framework for most of today's cybersecurity efforts. In the late 1990s, federal

[37] Department of Homeland Security Website, http://www.dhs.gov/files/programs/cybersecurity.shtm (emphasis added). This is a summary of *Protecting Our Federal Networks Against Cyber Attacks*, www.dhs.gov/files/programs/gc_1234200709381.shtm. The latter web page also provides details concerning how the DHS has focused its resources to prevent future attacks and intrusions.

[38] Department of Homeland Security, *Fact Sheet: Protecting Our Federal Networks Against Cyber Attacks*, Apr. 8, 2008, *available at* http://www.dhs.gov/xnews/releases/pr_12076 84277498.shtm.

[39] Department of Homeland Security, *Protecting Our Federal Networks Against Cyber Attacks*, www.dhs.gov/files/programs/gc_1234200709381.shtm. For more details on the CNCI, see John Rollins & Anna C. Henning, *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations* (Cong. Res. Serv. R40427), Mar. 10, 2009.

[40] Department of Homeland Security, *supra* note 39.

[41] *Id.*

[42] *Id.*

departments and agencies made extraordinary efforts to comply with PDD 63 by identifying critical assets, functions, and systems, as well as interdependencies among those critical assets, functions, and systems. The DHS continues that same effort today under new statutory and regulatory authorities, but today's efforts are essentially the PDD 63 process, embroiled in the same contentious debates that occurred during the implementation of PDD 63. The question of what constitutes a critical asset of national importance is an example of such debated issues. Following fourteen years of effort by the U.S. government, an effective cybersecurity program remains elusive.

III. THE GHOST OF CYBERSECURITY FUTURE

Developing an effective national cybersecurity program is an extraordinary challenge, especially in today's wired world of competing interests. For example, among all U.S. government agencies, the Department of Defense (DoD) is the most prolific agency on YouTube, and the White House has the most followers on Twitter and the most Facebook friends.[43] There are also five U.S. government sponsored virtual worlds created in Second Life, two by the National Aeronautics and Space Administration, one by the National Oceanic and Atmospheric Administration, one by the Centers for Disease Control and Prevention, and one jointly created by the Air Force, Navy, and Army.[44]

While use of social media improves collaboration, streamlines communications, costs little or nothing to use, potentially attracts young recruits into government service, and is highly portable, its use also creates a cybersecurity risk because social media make sensitive information publicly available on the Internet, complicate compliance with federal regulations, do not adhere to standards, put employee personal information at risk, and demand a lot of bandwidth.[45]

An effective national cybersecurity program requires – as stated in Executive Order 13,010, PDD 63, and subsequent initiatives – the *fully coordinated* authority and efforts of all federal departments and agencies, state and local governments, the private sector, and the international community.[46] Such a program must take into account the range of issues

[43] Brian Robinson, *Gov 3.0: The Future Revealed in 7 Lists*, FEDERAL COMPUTER WEEK, Sept. 7, 2009, *available at* http://fcw.com/Articles/2009/09/07/FED-LIST-FEATURE-LISTS.aspx.

[44] *Id.*

[45] *See* Doug Beizer & Amber Corrin, *5 Reasons Why DoD Should Embrace Social Media (and 5 Reasons Why Not)*, FEDERAL COMPUTER WEEK, Sept. 2, 2009, *available at* http://fcw.com/articles/2009/09/07/dod-and-web-2.aspx?s=fcwdaily_t140909.

[46] *See* Jeffrey Hunker, *U.S. International Policy for Cybersecurity: Five Issues That Won't Go Away*, 4 J. NAT'L SECURITY L. & POL'Y 195 (2010); Yasuhide Yamada et al., *A Comparative Study of the Information Security Policies of Japan and the United States*, 4 J.

raised by network monitoring, including, most importantly, constitutional concerns related to civil liberties and privacy.[47]

The interconnectivity of systems and networks demands that the federal program integrate and coordinate agency efforts. To date, no national coordinator has been given sufficient authority to develop and run an effective national cybersecurity program. It is problematic and unrealistic, of course, to expect that a national coordinator should have complete authority to *direct* the full integration, coordination, and operation of federal departments' and agencies' cybersecurity efforts, or complete regulatory authority over state and local governments and the private sector. However, the last fourteen years have demonstrated that a national coordinator with authority to direct only through consensus is likely to fail.

Thus the success of the U.S. cybersecurity program will depend upon whether the new national coordinator has more directive authority over federal departments and agencies and more regulatory authority over U.S. critical infrastructure and key resources than previous coordinators. Given resistance to change, the federal government may not allow a national coordinator to command complete directive and operational authority over federal information systems and regulatory authority over nonfederal information systems. It might require a catastrophic cyber incident to force change.

The *Cyberspace Policy Review* recommended that the President "consider appointing a cybersecurity policy official at the White House, reporting to the NSC and dual-hatted with the NEC, to coordinate the Nation's cybersecurity-related policies and activities."[48] It further recommends that to "be successful, the President's cybersecurity policy official must have clear presidential support, authority, and sufficient resources to operate effectively in the policy formulation and the coordination of interagency cybersecurity-related activities," but the recommendation makes it clear that a cybersecurity policy official "should not have operational responsibility or authority, nor the authority to make policy unilaterally."[49] This recommendation essentially mirrors the status quo and provides that the national coordinator has no authority even to establish policy, and in fact, has little more authority, if any more, than the DHS Secretary already has.

Two models, described below, provide insight as to what level of authority a national coordinator might require over federal departments and agencies to be effective. Regardless of which model is chosen, the existing regulatory authorities to set information security standards throughout the

NAT'L SECURITY L. & POL'Y 215 (2010)

[47] For a discussion of the civil liberties considerations raised by current cybersecurity proposals, see Gregory T. Nojeim, *Cybersecurity and Freedom on the Internet*, 4 J. NAT'L SECURITY L. & POL'Y 117 (2010).

[48] CYBERSPACE POLICY REVIEW, *supra* note 10, at 7.

[49] *Id.* at 7-8.

federal government should be consolidated and granted to the national coordinator.

The first model, the Commander of U.S. Strategic Command, helps us understand the level of authority that a national coordinator might require to direct network operations within federal departments and agencies. Within the DoD, the Commander of U.S. Strategic Command – currently acting through the Joint Task Force for Global Network Operations but in the future through a subunified U.S. Cyber Command – has the authority to direct the "operation and defense of the Global Information Grid to assure timely and secure Net-Centric capabilities across strategic, operational, and tactical boundaries in support of the DoD's full spectrum of war fighting, intelligence, and business missions."[50]

This concept of operations provides a "common framework and command and control" and combines the "disciplines of enterprise systems and network management, network defense, and information decision management."[51] This operational authority spans networks owned by military departments, Services, nine other combatant commands, and other DoD components, and has proven to be the most effective way for the DoD to defend and operate its networks. Similarly, giving the national coordinator such operational authority spanning federal networks might prove effective in regard to the federal information system.

If the decision is made not to grant the national coordinator authority to *direct* network operations across the federal government, we may look to another model, that of the Director of National Intelligence (DNI), to understand a different level of authority that a national coordinator might require to *coordinate* a U.S. government-wide cybersecurity program. The mission of the DNI is to provide superior information and analysis so as to give advantage in decisionmaking to policy makers, armed forces, homeland security officials, and law enforcement personnel. It does so by integrating foreign, military, and domestic intelligence capabilities and utilizing policy, personnel, and technology.[52]

By statute, the DNI's principal responsibilities are to serve as the head of the Intelligence Community and as the principal adviser to the President, the National Security Council (NSC), and the Homeland Security Council (HSC) for intelligence matters related to national security. The DNI is also responsible for overseeing and directing implementation of the National Intelligence Program.[53] The DNI's authorities must not "abrogate the

[50] U.S. Strategic Command Website, *Fact Sheet: Joint Task Force – Global Network Operations*, www.stratcom.mil/factsheets/gno/.

[51] *Id.*

[52] *See* Office of the Director of National Intelligence Website, *Vision and Mission*, www.dni.gov/mission.htm.

[53] 50 U.S.C. §403(b) (1949) (amended 2003).

statutory responsibilities of the heads of the departments of the United States Government."[54]

Nevertheless, the DNI has authorities for budget, transfer and reprogramming of funds, and the formal tasking that allow the DNI to fulfill the office's responsibilities.[55] In like manner, a director of national cybersecurity could serve as: head of the federal information security community; principal adviser to the President, the National Security Council, and the Homeland Security Council for cybersecurity matters related to national security; and be responsible for overseeing and directing implementation of the national cybersecurity program.

The authorities represented by both models may be blended to empower the national coordinator. In sum, to be effective, a national coordinator needs authority sufficient to do the following:

- Conduct network operations across federal departments and agencies.
- Develop and direct participation in a national cybersecurity program that includes required participation, for example, in the CNCI and the Einstein Program.
- Establish information security standards for federal departments and agencies that will also serve as best business practices for the private sector.
- Direct research and development of new cybersecurity technologies.

Because U.S. national security is critically dependent on cyberspace, where the United States faces a "growing array of cyber threats and vulnerabilities," the Secretary of the DoD has directed the Commander of U.S. Strategic Command to establish a subunified U.S. Cyber Command. The U.S. Cyber Command "will coordinate computer-network defense and direct U.S. cyber-attack operations" and support to civil authorities with cybersecurity.[56] The Secretary of the DoD plans to nominate the Director of the National Security Agency (NSA) to command the U.S. Cyber Command.[57] Although some have raised alarms concerning the role of the NSA in cybersecurity, the Director of the NSA has explained publicly that the U.S. Cyber Command will adopt a team approach that "would give the NSA lead responsibility for protecting military and intelligence networks

[54] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638.

[55] 50 U.S.C. §403-1 (1949) (amended 2003).

[56] Siobhan Gorman, *Gates To Nominate NSA Chief To Head New Cyber Command*, WALL ST. J., Apr. 24, 2009, at A4.

[57] *Id.*

while the Department of Homeland Security works to protect other government networks."[58]

The Deputy Secretary of the DoD has also made clear that the mission of the U.S. Cyber Command would be to protect and defend our defense and military networks and that the responsibility for protecting federal civilian networks would remain with the DHS.[59] The Deputy Secretary stated that in the future, the effectiveness of U.S. cybersecurity will depend on how the United States answers key questions, such as how we develop an effective deterrence strategy, organize government as a whole, cooperate internationally, partner with the private sector, and define the "rules of the road" within the DoD for cyberspace operations.[60]

The question as to what rules ought to govern DoD cyberspace operations posed by the Deputy Secretary gets at interesting issues.[61] First, public statements establish that the mission of the U.S. Cyber Command is to protect and defend DoD networks, and that the DoD will serve in a supporting role to the DHS in helping that Department defend non-DoD federal information systems.[62] However, the mission of the DoD is to defend the United States. One very important rule of the road ripe for public debate[63] concerns the question of when potential consequences of a cyber event for federal departments and agencies rise to the level that the DoD should no longer play a supporting role to the DHS but should serve the primary role in defending the United States. Another very important rule of the road ripe for public debate concerns when the potential

[58] *See, e.g.,* Siobhan Gorman & Yochi J. Dreazen, *New Military Command To Focus on Cybersecurity*, WALL ST. J., Apr. 22, 2009, at A2. For a discussion of oversight mechanisms implemented within the NSA to safeguard civil liberties and privacy, see John N. Greer, *Square Legal Pegs in Round Cyber Holes: The NSA, Lawfulness, and the Protection of Privacy Rights and Civil Liberties in Cyberspace*, 4 J. NAT'L SECURITY L. & POL'Y 137 (2010).

[59] Remarks of William J. Lynn III, Deputy Secretary of Defense, *Protecting the Domain: Cybersecurity as a Defense Priority,* before the Center for Strategic and International Studies, June 15, 2009, *available at* http://www.defense.gov/Transcripts/Transcript.aspx?TranscriptID=4433.

[60] *Id.*

[61] *See, e.g.*, MICHAEL N. SCHMITT & BRIAN T. O'DONNELL, COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW (International Law Studies Bluebook Series Vol. 76, 2002). This Naval War College Blue Book provides more than 450 pages of discussion concerning international legal and policy implications of computer network attack. The Appendix to this Blue Book also contains *An Assessment of International Legal Issues in Information Operations*, a 70-page analysis by the U.S. Department of Defense Office of General Counsel updated in November 1999.

[62] Such support is normally provided under the authority of 10 U.S.C. §§371-382 (2006), *Military Support for Civilian Law Enforcement Agencies*, or 31 U.S.C. §1535 (2006), *Economy Act.*

[63] It is very important that a debate concerning the general role of the DoD to defend U.S. cyberspace be public, recognizing, of course, that the specific rules authorizing a use of force in self-defense will be classified and not publicly available.

consequences of a cyber event for U.S. critical infrastructure, key resources, or private sector elements justify a decision that the DoD should take action to defend the United States.

Indeed, both of these questions have already been raised publicly as a result of the distributed denial of service attacks over the weekend of July 4, 2009.[64] Specifically, the public is beginning to ask what "are the appropriate actions for individuals and countries to take in response to different types of computer attacks," what "should the rules of engagement be for the military to use cyber weapons," and when could a cyberattack "warrant a cyber response or kinetic military reaction?"[65]

Constitutionally, only the President can authorize the DoD to use force in defense of the United States. A national coordinator, however, should initiate a public debate among federal departments and agencies and the U.S. public, and make a recommendation to the President as part of a comprehensive national cybersecurity plan as to what role the DoD should serve in defending non-DoD federal information systems and U.S. critical infrastructure and key resources. This recommendation should also take into account the role of the U.S. Congress in any cyber use of force policy, which is discussed later in this journal issue.[66] A national cybersecurity plan should also address the potentially critical role of the U.S. National Guard. Given their unique set of authorities to perform duties under the laws of the states of the United States or under their federal service, the U.S. National Guard could perform a vital cybersecurity mission by providing a bridge for coordination between state governments and the federal government.

CONCLUSION

If the U.S. government continues to address the cyber threat by simply maintaining today's inadequate framework of dispersed and uncoordinated authorities and responsibilities, then the Ghosts of Cybersecurity Past and Present tell us that its efforts are doomed to fail. The powerful lesson of Charles Dickens's *A Christmas Carol*, however, is that we can change our future, that we can learn and evolve through an acquired self-awareness and understanding of the past, present, and future. My theme evoking the spirit of Christmas past, present, and future was chosen to be a bit light hearted, since cybersecurity is such a serious and complex issue. Our vision of how

[64] Ben Bain, *Cyberattacks Add Fuel to Cybersecurity Debate*, FEDERAL COMPUTER WEEK, July 10, 2009, *available at* http://fcw.com/articles/2009/07/10/cyberattacks-prompt-cybersecurity-debate.aspx.

[65] *Id.* For discussions concerning a use of force in cyberspace and the rules that apply, see Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L SECURITY L. & POL'Y 61 (2010), and David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SECURITY L. & POL'Y 85 (2010).

[66] Stephen Dycus, *Congress's Role in Cyber Warfare*, 4 J. NAT'L SECURITY L. & POL'Y 153 (2010).

to move forward has been clouded, not by greed as was the case with Ebenezer Scrooge, but by a sense of being overwhelmed by the size and complexity of the cyber threat. However overwhelming and complex the cyber threat may be, the way ahead may be easier than most think.

The United States has long identified and has in place the basic elements of at least eighty percent of the solution for effective cybersecurity, as we understand it through our past and present experiences. These elements remain segregated – despite the efforts of Executive Order 13,010, PDD 63, HSPD-7, and the CNCI. What the United States needs is a national coordinator with the vision and authority to unify and integrate the elements of that eighty percent solution and then identify the remaining twenty percent as we evolve and learn how to incorporate every citizen as a part of the solution. This theme is reflected in this issue's title – *National Leadership, Individual Responsibility*. Once the right balance of authority is determined for a national coordinator, that role must also be institutionalized in law to create and maintain stability and momentum – elements frequently lost due to changes in priorities.

The remaining twenty percent of the solution will most likely turn out to be central for effective cybersecurity. For example, cybersecurity initiatives that leverage the confluence of biometrics and identity management may very well establish a critical foundation for attribution and security. Internet service providers could change their user agreements to require users to authorize their service providers to run programs on users' machines that will identify and clean malicious software and thus significantly reduce the effectiveness of botnets and distributed denial of service attacks. Such agreements would be value-added for the user and no more invasive or intrusive than antivirus or other security programs. Similarly, Internet service providers could be required by law or regulation, depending on the circumstances or requirements, to participate in a cyber incident information sharing arrangement, or to provide data to an early warning system that helps everyone defend their information systems and networks.

The abuse of the Internet for terrorist purposes such as for radicalization, recruitment, training, operational planning, and fundraising should be aggressively criminalized and prosecuted. Internet service providers should have a statutory duty to prevent their servers and networks from being used for such criminal activities.

Technology will improve in a way that will significantly reduce the cyber threat to U.S. national security and strengthen our ability to respond in self-defense. The pervasive and pernicious nature of the cyber threat caused by the open architecture of the Internet and the extraordinary number of interdependencies that permeate all U.S. government and private sector information systems demand that we revisit our notions of sovereign federal departments and agencies that have complete independence from any authority other than that of the President. However, the single most important missing element for an effective national cybersecurity plan is a coordinator with the vision and authority to move beyond today's existing framework and to make a difference in our nation's cybersecurity.