# Introduction

William C. Banks[*] & Elizabeth Rindskopf Parker[**]

For many of us, the cyber threat to U. S. national security is amorphous and not easy to comprehend. At the same time, in the last two years of the Bush administration and through the first year of the Obama presidency, cybersecurity has been characterized as "one of the most urgent national security problems facing the new administration."[1] Our cyber systems have increasingly been infiltrated in recent years by malefactors with widely ranging motivations and associations. Experts point to stunning amounts of sensitive material lost to cyber thieves.

Given the increasing dependence on cyber technology, the vulnerabilities within insecure cyber networks are hard to quantify and even harder to understand and protect against. We have devoted the current issue of the *Journal of National Security Law & Policy* (JNSLP) to cyber threats in an attempt to raise awareness and focus national debate on what should be done in a variety of contexts to improve cybersecurity.

Many have helped in this project, but particular thanks go to Gary Sharp, special editor for this issue, who conceived the idea and did much to shape its content. Thanks are also due to Richard Shiffrin, who graciously served as an unofficial editor of this special issue, reviewing and critiquing significant amounts of material.

For many reasons, the collection of views presented in this issue is especially timely. By any measure, developing and implementing a forward-looking cybersecurity policy is among the most compelling items on the Obama administration national security agenda. It may also be the most complex. Developing such a policy requires a sophisticated understanding of the technology, interests, and motivations involved in perpetrating cyber attacks, on the one hand, and an appreciation of the tradeoffs implicated in decisions to create new authorities and institutional arrangements for cyber defense, on the other. That the Administration has not yet implemented a blueprint for action, despite the issue's priority, may simply reflect its understanding that, given the intricacies of the threat and its management, leadership means showing restraint, rather than acting precipitately.

---

[*] Director, Institute for National Security and Counterterrorism; Board of Advisors Distinguished Professor of Law, Professor of Public Administration, Syracuse University; Editor-in-Chief, *Journal of National Security Law & Policy*.

[**] Dean, University of the Pacific, McGeorge School of Law; founding Editorial Board Member, *Journal of National Security Law & Policy*.

1. *See* CENTER FOR STRATEGIC & INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY (2008), *available at* http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

Indeed, if the answers were clear-cut, there would be no need for the extensive research and discussion found in the pages that follow. This JNSLP issue follows a series of excellent studies exploring cyber issues from the perspectives of the offensive use of cyber weapons and the dynamics of assuring an effective defense against cyber attacks. The first studies came out in the 1990s, a time when the world was developing technologies enabling individuals to connect on global projects – some benign, some not so benign. The United States and its allies – and our enemies, as well – developed and deployed computerized tools to conduct a new kind of war. In the late 1990s, a team of Department of Defense lawyers undertook studies of the implications for domestic and international law of such information operations.[2] There were a number of other studies in the 1990s, including *Critical Foundations: Protecting America's Infrastructures*.[3] However, only in the last few years has there been serious treatment of cyber issues by scholars and practitioners.[4]

More recently, in January 2008, the Bush administration initiated the Comprehensive National Cybersecurity Initiative (CNCI).[5] As conceived by classified presidential directives, the CNCI established "the policy, strategy, and guidelines to secure federal systems," while it prescribed "an approach that anticipates future cyber threats and technologies, and requires the federal government to integrate many of its technical and organizational capabilities to better address sophisticated threats and vulnerabilities."[6]

---

2. AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS (1999), *available at* http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf.

3. ROBERT T. MARSH, CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES (1997), *available at* http://fas.org/sgp/library/pccip.pdf.

4. *See, e.g.*, NATIONAL RESEARCH COUNCIL, TOWARD A SAFER AND MORE SECURE CYBERSPACE (Seymour E. Goodman & Herbert S. Lin eds., Nat'l Acad. Press, 2007); CYBERPOWER AND NATIONAL SECURITY (Franklin D. Kramer, Stuart H. Starr & Larry K. Wentz eds., 2009); NATIONAL RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES (William A. Owens, Kenneth W. Dam, & Herbert S. Lin, Nat'l Acad. Press, 2009); John Rollins & Anna C. Henning, *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations* (Cong. Res. Serv. R40427), Mar. 10, 2009; *National Security Threats in Cyberspace* (ABA Standing Committee on Law and National Security and National Strategy Forum, Sept. 2009), *available at* http://www. abanet.org/natsecurity/threats_%20in_cybers pace.pdf; MARTIN C. LIBICKI, CYBERDETERRENCE AND CYBERWAR (2009), *available at* http://www.rand.org/pubs/mono graphs/MG877/; CENTER FOR STRATEGIC & INT'L STUDIES, IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR (2010).

5. THE COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE (declassified summary), *available at* http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

6. Department of Homeland Security Fact Sheet: DHS 2008 End of Year Accomplishments (Dec. 18, 2008), *available at* http://www.dhs.gov.xnews/releases/pr_1229 609413187.shtm.

In May 2009, the Obama administration established a Cyberspace Policy Review,[7] and in December 2009, the White House appointed a Cybersecurity Coordinator to lead the federal cyber response.[8] Yet there has been no clear or single articulation of a cybersecurity policy. Nor has there been an agreed-upon framework for leadership and implementation of any policy that may be developed.

In the absence of a cyber policy, the United States has principally relied upon law enforcement and computer crimes statutes, which empower federal, state, and local officials to investigate and punish malfeasance in the cyber domain. The efficacy of this approach is questionable, for a number of reasons. For one, the transnational nature of cyber activities limits considerably the effectiveness of any one nation's domestic law enforcement strategies to combat cyber crime.

As the United States worked to combat illicit cyber activities through law enforcement methods, it also developed on an *ad hoc* basis over the last two decades various organizational structures in response to the cyber threat. Yet those infrastructure protection boards and cyber commissions typically lacked leadership, had no real authority, and were often made up of individuals who did not have sufficient expertise in the full range of necessary specialties, including national security, cyber security, policy, and law.

Meanwhile, the private sector, owners of most of our critical cyber infrastructure, pursued an unstructured response to the threats, relying in the first instance on government systems for cyber security.

As the Obama administration launched its Cyberspace Policy Review, Director of National Intelligence Dennis Blair testified to the Senate Intelligence Committee that:

> Growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructures. . . . A successful attack against a major financial service provider could severely impact the national economy, while cyber attacks against physical infrastructure computer systems such as those that control power grids or oil refineries have the potential to disrupt services for hours or weeks.[9]

---

7. 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.

8. On December 22, 2009, the White House appointed a Cybersecurity Coordinator, Howard Schmidt. *See* Ellen Nakashima & Debbi Wilgoren, *Obama To Name Former Bush, Microsoft Official as Cyber-Czar*, WASH. POST, Dec. 22, 2009, at A04.

9. U.S. Congress, Senate Select Comm. on Intelligence, Annual Threat Assessment

Amidst the growing awareness of our vulnerabilities and the increasing likelihood of cyber intrusions affecting our national security, federal agencies and members of Congress fretted that existing authorities did not enable an effective cybersecurity defense. Proposals for legislation that would invigorate cyber defense as a responsibility of the Department of Homeland Security compete with those that would vest the National Security Agency with those roles and missions.

More is at stake here than questions of bureaucratic turf. The question of control raises a fundamental issue for our democracy: Will we vest responsibility for cybersecurity in domestic matters with a premier foreign intelligence agency such as NSA, or should we place responsibility in a domestic department such as the DHS, where technical competence is a yet untested? At the same time, none of the federal government prescriptions to date has fully incorporated ways to cooperate with private sector and other nonfederal organizations.

As cyber events have become more serious and frequent in recent years, investments in and writing about cybersecurity also increased. This JNSLP symposium reflects this turn. Our authors include current and former government insiders, including some working on the very issues under discussion. We challenged them to address the largest and most difficult issues and suggest answers to interrelated questions, such as:

- How should we best organize our government to act?
- What implementation mechanisms best achieve the policy objectives?
- Should the structure be built from the top down, or from the bottom up?
- Would a series of partnerships between government, corporate, and private stakeholders better secure the Internet?

Many of the articles that follow are provocative, and deliberately so. The authors share their experiences and insights, and they suggest prescriptions, widely different from one another. They explore the uses and potential abuses of cyber devices as weapons, particular problems of civil liberties and privacy, international and comparative policies on the Internet, and the role of Congress in managing any potential cyberwar.

---

of the Intelligence Community: Hearing on the Threats to the Nation, 111th Cong. (Feb. 12, 2009).

In sum, if one thing is clear about the state of cybersecurity in the United States, it is that there is not now an agreed-upon way forward. There is, however, widespread consensus that cyber threats are growing faster than our ability to thwart them, and that the risk we face by failure to act is of monumental proportion.